MASTER'S THESIS

Verschillen in grondigheid van GDPR-implementatie tussen de publieke en private sector

Horlings, R.A. (Roeland)

Award date:
2020

Verschillen in grondigheid van GDPR-implementatie tussen de publieke en private sector

Differences in symbolic vs substantive GDPR-implementation for the public vs private sector

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Master Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT IM9806 Afstudeertraject Business Process Management & IT
Student:	R.A. Horlings
Identiteitsnummer:	
Datum:	April 2020
Afstudeerbegeleider	dr. L. Bollen
Meelezer	dr. R. Bosua
Derde beoordelaar	<indien aanwezig>
Versie nummer:	1.0
Status:	Definitieve versie

Abstract

De grondigheid van GDPR-implementaties van de publieke en de private sector worden in dit onderzoek gemeten op basis van beschikbare factoren uit openbare bronnen. Dit leidt tot een score die de organisaties en sectoren plaatst op een schaal van symbolisch tot grondig. De gebruikte bronnen zijn organisatiewebsites, privacyverklaringen en jaarverslagen. Naast het onderscheid tussen de publieke en private sector wordt ook de organisatiegrootte als selectievariabele meegenomen. Uit de resultaten wordt geconcludeerd dat de GDPR-implementatie door de private sector grondiger is dan die van de publieke sector. Dit heeft mogelijk te maken met de wijze waarop de publieke sector hun privacyverklaringen vormgeeft, omdat hier structureel lager wordt gescoord door het niet volledig benoemen van privacyrechten. Ook blijken organisaties moeite hebben met de wijze waarop zij de GDPR moeten interpreteren en implementeren, gezien de onduidelijkheid over privacyrechten in hun communicatie. Aanbevelingen zijn onder meer het gebruik van (volledige) templates voor privacyverklaringen en het besteden van meer aandacht aan privacy in jaarverslagen.

Sleutelbegrippen

GDPR; Privacy; Overheid; Publieke sector; Private sector; Symbolic vs substantive; Symbolisch vs grondig.

Samenvatting

Sinds 25 mei 2018 is er voor de lidstaten van de Europese Unie nieuwe privacywetgeving van kracht gegaan. Met de *General Data Protection Regulation* (GDPR), in het Nederlands de *Algemene Verordening Gegevensbescherming* (AVG), zijn de privacyrechten van personen versterkt en uitgebreid en liggen er meer verantwoordelijkheden bij organisaties op gebied van data- en privacybescherming. Ondanks een aanloopfase van twee jaar en het risico op hoge boetes, bleek dat veel organisaties niet klaar waren voor deze nieuwe privacywetgeving.

De *Autoriteit Persoonsgegevens* (AP), die als toezichthouder in Nederland de bescherming van persoonsgegevens bewaakt, had ook geen vlekkeloze aanloop. Wat ertoe heeft geleid dat in de eerste jaren dat de GDPR van kracht is, de focus voor controle vanuit de AP voornamelijk is gericht op overheidsorganisaties en zorginstellingen.

Gezien deze ontwikkelingen richt dit onderzoek zich op de mate van grondigheid waarmee organisaties de GDPR hebben geïmplementeerd. Waarbij met name het verschil in grondigheid tussen de publieke en private sector wordt belicht. Verder wordt de organisatiegrootte in dit onderzoek meegenomen.

De grondigheid van GDPR-implementatie wordt in dit kwantitatieve onderzoek vastgesteld als een score. Die score wordt behaald door te voldoen aan factoren die vanuit openbare bronnen beoordeeld worden. Als bronnen worden privacyverklaringen en jaarverslagen van organisaties gebruikt. In de privacyverklaringen wordt geanalyseerd welke privacyrechten met lezers worden gedeeld en in de jaarverslagen wordt de aandacht voor privacywetgeving gemeten.

Hiervoor zijn 152 organisaties onderzocht binnen de sectoren publiek, privaat en semipubliek. De private sector scoort daarvan het hoogst voor grondigheid van GDPR-implementaties, met daarna de semipublieke sector en ten slotte de publieke sector die het laagst scoort. Hoewel de organisatiegrootte een significante invloed heeft op de score die organisaties behalen, was dit als modererend effect in de interactie met de sector niet significant.

Uit de resultaten wordt geconcludeerd dat de GDPR-implementatie door de private sector grondiger is dan die van de publieke sector. Dit heeft mogelijk te maken met de wijze waarop de publieke sector hun privacyverklaringen vormgeeft, omdat hier structureel lager wordt gescoord door het niet volledig benoemen van privacyrechten. Ook blijken organisaties moeite te hebben met de wijze waarop zij de GDPR moeten interpreteren en implementeren, gezien de onduidelijkheid over privacyrechten in hun communicatie.

Dit onderzoek heeft als voornaamste aanbeveling voor de praktijk om best practices/templates te gebruiken voor het opstellen van privacyverklaringen. Benoem daarbij als organisatie ook de privacyrechten die minder of niet van toepassing zijn. Besteed daarnaast aandacht aan privacy in jaarverslagen, zodat organisaties uitgedragen hoe zij over privacy denken en op welke manier zij hiermee bezig zijn. Ten slotte kunnen organisaties voorbeelden delen van de wijze waarop de GDPR geïmplementeerd kan worden. Zodat er een norm ontstaat die andere organisaties kunnen volgen.

De voornaamste aanbeveling voor verder onderzoek is om de koppeling te leggen tussen kwalitatieve kenmerken van GDPR-implementaties en de factoren die vanuit publieke bronnen meetbaar zijn. Verder is meer onderzoek nodig naar de GDPR en de implementatiestrategieën hiervan, aangezien de GDPR relatief recent van kracht is. Daarnaast is verder onderzoek naar meer specifieke variabelen nodig, zodat ingezoomd kan worden op meer precieze factoren die invloed hebben op de grondigheid van GDPR-implementaties.

Summary

Since May 25th, 2018, new privacy legislation has come into effect for the member states of the European Union. With the General Data Protection Regulation (GDPR), the privacy rights of individuals have been expanded and responsibilities for organizations in the field of data and privacy protection have increased. Despite a two-year run-up phase and the risk of high fines, it turned out that many organizations were not ready for this new privacy legislation.

The preparation of the Dutch Data Protection Authority (AP), which monitors the protection of personal data as a supervisory authority in the Netherlands, was also not flawless. As a result, in the first years that the GDPR came into effect, the focus for control from the AP is mainly aimed at government organizations and healthcare institutions.

In view of these developments, this study focuses on the degree of thoroughness with which organizations have implemented the GDPR. Where the focus will be the difference between the public and private sector. Besides the sector, the organizational size is also included in this study.

The thoroughness of GDPR implementation is determined as a score in this quantitative study. This score is achieved by complying with factors that are assessed from public sources. Privacy statements and annual reports of organizations are used as sources. The privacy statements analyze which privacy rights are shared with readers and the annual reports measure the attention paid to privacy legislation.

152 organizations were assessed for this within the public, private and semi-public sector. The private sector scores highest for the thoroughness of GDPR implementations, followed by the semi-public sector and finally the public sector has the lowest score. Although the size of the organization has a significant influence on the score that organizations achieve, this was not significant as a moderating effect in the interaction with the sector.

The results conclude that the GDPR implementation by the private sector is more thorough than that of the public sector. This has been made possible by the way in which the public sector designs their privacy statements, because here they score structurally lower due to the incomplete naming of privacy rights. Organizations also appear to have difficulties with the way in which they must interpret and implement the GDPR, given the lack of clarity about privacy rights in their communication.

The main recommendation of this study is to use best practices / templates for composing privacy statements. As an organization, also mention those privacy rights that are less applicable or not applicable at all. In addition, pay attention to privacy in annual reports, so that organizations propagate what their stance on privacy is and which steps they are taking to get there. Finally, organizations can provide examples of how the GDPR can be implemented. So a standard is created that other organizations can follow.

The main recommendation for further research is to link the qualitative characteristics of GDPR implementations with the factors that can be measured from public sources. Furthermore, more research is needed into the GDPR and its implementation strategies, since the GDPR has been in effect relatively recently. In addition, further research into more specific variables is needed so that we can zoom in on more precise factors that affect the thoroughness of GDPR implementations.

Inhoudsopgave

Abstract ii
Sleutelbegrippen ii
Samenvatting iii
Summary iv
Inhoudsopgave v
1. Introductie 1
1.1. Achtergrond 1
1.2. Gebiedsverkenning 2
1.3. Probleemstelling 2
1.4. Opdrachtformulering 3
1.5. Motivatie/relevantie 3
1.6. Aanpak in hoofdlijnen 4
2. Theoretisch kader 4
2.1. Onderzoeksaanpak 4
2.1.1. Doel van theoretisch kader 4
2.2. Uitvoering 5
2.3. Resultaten en conclusies 5
2.3.1. Onderscheid publieke en private sector 6
2.3.2. Symbolisch versus grondig 8
2.3.3. Privacy(wetgeving) 8
2.3.4. Maatregelen en factoren GDPR 9
2.4. Doel van het vervolgonderzoek 10
2.4.1. Onderzoeksmodel 10
2.4.2. Hypotheses 11
3. Methodologie 11
3.1. Conceptueel ontwerp: keuze van onderzoeksmethode(n) 11
3.2. Technisch ontwerp: uitwerking van de methode 13
3.2.1. Organisaties 13
3.2.2. Bronnen 13
3.2.3. Factoren en maatregelen GDPR 13
3.3. Gegevensanalyse 14
3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten 15
3.4.1. Validiteit 15

3.4.2. Betrouwbaarheid 15
3.4.3. Ethische verantwoording 15
4. Resultaten 16
4.1. Uitvoering onderzoek 16
4.2. Resultaten 16
5. Conclusie, discussie en aanbevelingen 21
5.1. Conclusie 21
5.2. Discussie – reflectie 22
5.3. Aanbevelingen voor de praktijk 23
5.4. Aanbevelingen voor verder onderzoek 24
6. Referenties 25
7. Appendices 27
7.1. Appendix 1: Onderzoeksaanpak 27
7.2. Appendix 2: Selectie van organisaties 29
7.3. Appendix 3: Dataverzameling scoreprotocol 30

1. Introductie

1.1. Achtergrond

Sinds de Europese verordening *General Data Protection Regulation* (GDPR) op 25 mei 2018 van kracht is, hebben organisaties binnen de EU zich aan strengere wetgeving op gebied van data- en privacybescherming te houden. In het Nederlands spreken we als we het hebben over de GDPR over de *Algemene Verordening Gegevensbescherming* (AVG). In dit onderzoek wordt er gerefereerd naar deze verordening met de Europese benaming, de GDPR, omdat dit de internationale context van de wetgeving beter weergeeft.

Nadat deze verordening op 24 mei 2016 in werking is getreden, kregen organisaties twee jaar de tijd om hun bedrijfsvoering met de GDPR in overeenstemming te brengen. Die periode was bedoeld om de implicaties van de GDPR voor de organisatie in beeld te krijgen en hierop de benodigde maatregelen te nemen. Na deze aanloopperiode van twee jaar moesten alle Europese organisaties voldoen aan de voorwaarden die in de GDPR worden gesteld.

Ondanks mogelijke negatieve consequenties van niet voldoen aan de GDPR, zoals het risico op hoge boetes, was tegen de deadline bij veel organisaties duidelijk dat zij niet compliant waren. Zo bleek dat in januari 2018, slechts maanden verwijderd van de deadline, van vijfhonderd onderzochte Londense organisaties bijna een kwart zich niet bewust was van de GDPR (London Chamber of Commerce and Industry, 2018). Een groot aantal organisaties lieten hun voorbereiding – als daar al sprake van was – tot het laatste moment liggen (Garber, 2018).

Ook de handhaving door de Autoriteit Persoonsgegevens (AP) had geen vlekkeloze aanloop (Mebius, 2018). Er was sprake van interne onrust en onderbezetting bij de AP. Met als gevolg dat tijdens de eerste jaren dat de GDPR van kracht is, de focus zal liggen op handhaving bij overheids- en zorgorganisaties. Daarmee hoeft het bedrijfsleven deze periode nog niet te vrezen voor strikte handhaving vanuit de AP.

Nu deze deadline enige tijd achter ons ligt, is de vraag waar de meeste organisaties op dit moment staan in hun implementatie van GDPR-maatregelen. Het blijkt dat sommige organisaties ruim na het van kracht gaan van de GDPR nog tegen zaken aanlopen als verouderde systemen die compliance bemoeilijken (Hofmans, 2019) en maatregelen die werkzaamheden ernstig belemmeren (de Vries & Sys, 2019).

Compliance aan een verordening is niet optioneel, dus van organisaties wordt verwacht dat zij volledig aan de GDPR voldoen. Desondanks zitten er gezien de nieuwsberichten behoorlijke verschillen in de mate waarin organisaties de GDPR momenteel hebben geïmplementeerd.

De huidige aanpak in handhaving van de AP richt zich voorlopig voornamelijk op overheidsorganisaties (Mebius, 2018). Deze keuze wordt gemotiveerd met de redenen dat er in de publieke sector veel met gevoelige persoonsgegevens wordt gewerkt en dat de publieke sector in het volgen van privacywetgeving een voorbeeldfunctie heeft.

Gezien de relatief recente invoering van de GDPR en de vraagtekens rond compliance binnen zowel de publieke als private sector, richt dit onderzoek op de grondigheid van GDPR-implementaties.

Binnen deze sectoren wordt in dit onderzoek onderscheid gemaakt tussen:

- Publieke sector (overheidsorganisaties)
- Semipublieke sector (semioverheidsorganisaties);
- Private sector (particuliere organisaties/bedrijfsleven).

De semipublieke sector is voor dit onderzoek niet van het grootste belang, en zal daarom niet elke keer worden vermeld als het gaat over de verschillen en overeenkomsten tussen de sectoren. De semipublieke sector komt wel expliciet terug in de keuze voor te onderzoeken organisaties en in de onderzoeksresultaten.

Het doel van dit onderzoek is om meer inzicht te bieden in de grondigheid van GDPR-implementaties, met als focus op verschillen in grondigheid tussen de publieke en private sector. Gezien de GDPR recent van kracht is gegaan, is over de implementatie hiervan weinig onderzoek gedaan. Daarnaast is het verschil tussen de publieke en private sector van belang omdat hier volgens nieuwsberichten een groot verschil in voorbereiding en implementatie van de GDPR. De uitkomsten van tonen aan in welke mate de sector invloed heeft op de grondigheid van GDPR-implementaties.

De opbouw van dit onderzoek start met het theoretisch kader, waarin eerder onderzoek wordt aangehaald op het gebied van onder meer GDPR, privacy en publiek vs privaat. Uit het theoretisch kader wordt bepaald met welke factoren de grondigheid van een GDPR-implementatie kan worden gemeten. Er worden een onderzoeksmodel en hypotheses opgesteld. Daarna wordt in de methodologie beschreven op welke de wijze de data zal worden verzameld en geanalyseerd.

Vervolgens wordt uit publiek beschikbare bronnen data verzameld en geanalyseerd. Hieruit vormt zich een beeld dat aantoont of er tussen de publieke en de private sector op basis van de onderzochte factoren een wezenlijk verschil is in de grondigheid van implementaties van de GDPR. Met tot slotte conclusies, de reflectie en aanbevelingen voor de praktijk en voor verder onderzoek.

1.2. Gebiedsverkenning

In het kader van de GDPR wordt veel gesproken over data- en privacybescherming. In de GDPR worden regels vastgesteld over de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens. Met deze regels worden fundamentele vrijheden op gebied van privacy beschermd. De wijze waarop de GDPR is opgesteld geeft hiervoor aan wat er gedaan moet worden, maar voorschrijft niet hoe het gedaan moet worden (Garber, Joe, 2018).

Daarmee is de interpretatie van de benodigde maatregelen voor de GDPR een punt van aandacht in dit onderzoek. In het theoretisch kader wordt een inschatting gemaakt welke factoren indicatief zijn voor een grondige GDPR-implementatie.

1.3. Probleemstelling

Organisaties hebben aanzienlijke veranderingen moeten doorgaan in het verwerven, bewaren, verwerken en delen van persoonsgegevens. Dit heeft invloed gehad op de wijze waarop deze organisaties hun processen inrichten en hoe zij persoonsgegevens bewaren en beschermen. Zowel bedrijfsmatig als technisch is dit in veel gevallen een ingrijpende en kostbare omslag. Dat leidt ertoe dat maatregelen om aan deze nieuwe wetgeving te voldoen niet per definitie grondig worden doorgevoerd. Dit onderzoek biedt inzicht in verschillen in grondigheid waarmee de publieke en private sector de GDPR hebben geïmplementeerd.

1.4. Opdrachtformulering

De hoofdvraag van dit onderzoek is:

- *Hoeverre is de sector waartoe een organisatie behoort (publiek/semipubliek/privaat) voorspellend voor de mate van grondigheid in hun GDPR-implementatie?*

Deelvragen om deze hoofdvraag te beantwoorden zijn:

- *Hoe wordt het onderscheid tussen de publieke en private sector bepaald?*
- *Met welke factoren kan de grondigheid van een GDPR-implementatie worden bepaald?*
- *Hoe kan informatie over deze factoren worden verzameld en gemeten uit openbare bronnen?*

Allereerst moet er een overzicht worden gecreëerd van de te onderzoeken organisaties en de sector waartoe zij behoren. Er wordt onderzocht welke maatregelen de GDPR met zich meebrengt, en wat voor factoren daarvan uit openbare bronnen te meten zijn. Verder wordt een verkenning gedaan naar eerder onderzoek over privacy, GDPR, het onderscheid tussen de publieke en de private sector en theorieën om de later verkregen resultaten te voorspellen en te verklaren.

Aangezien dit een kwantitatief onderzoek betreft, worden uitkomsten voornamelijk verklaard uit huidige literatuur en gevestigde theorieën. Het valideren of de gemeten factoren in de praktijk aansluiten op een symbolische of grondige GDPR-implementatie valt buitende scope van dit onderzoek.

1.5. Motivatie/relevantie

De GDPR is door de recente invoering van deze verordening een actueel onderwerp. Hoe organisaties met persoonsgegevens omgaan en wat ze daarmee mogen doen, is een onderwerp dat politiek en maatschappelijk op veel aandacht mag rekenen.

Dit onderzoek toont de mate van grondigheid waarmee sectoren de GDPR hebben geïmplementeerd en kan daarnaast inzicht bieden in de problemen waar organisaties tegenaan lopen bij de implementatie van de GDPR. Bijvoorbeeld als blijkt dat veel organisaties moeite hebben om bepaalde maatregelen te implementeren. Dit kan wijzen op bijvoorbeeld moeilijkheden in implementatie, denk daarbij aan hoge kosten of ingewikkelde systeemwijzigingen, of conflicterende belangen, zoals wanneer het gebruik van persoonsgegevens is vervlochten met de bedrijfs- en informatieprocessen die een organisatie hanteert. Aangezien in de inhoudelijke oorzaken van uitkomsten geen inzicht is, worden hierover eventueel aanbevelingen gedaan voor vervolgonderzoek.

Het onderscheid tussen de publieke en private sector wordt gemaakt om meerdere redenen. Ten eerste omdat bij de Autoriteit Persoonsgegevens, de handhaver op gebied van Privacy en GDPR in Nederland, een onderscheid wordt gemaakt in handhaving tussen deze sectoren. Daarin wordt specifiek gerefereerd aan de belangrijke informatiepositie en de voorbeeldfunctie die van de overheid verwacht wordt in het naleven van de GDPR (Autoriteit Persoonsgegevens, AP doet handreikingen om registratie datalekken te verbeteren, 2018). Dit veronderstelt een verschil in naleving van de GDPR tussen de publieke en private sector.

Verder is dit onderscheid relevant omdat er nog weinig onderzoek is gedaan in de richting van implementaties van de GDPR, waardoor een onderzoek naar de verschillen tussen deze brede en

eenvoudig te identificeren sectoren inzicht geeft in verschillen in implementatie die duidelijk aanwijsbaar en te generaliseren zijn.

1.6. Aanpak in hoofdlijnen

Aan de basis van dit onderzoek liggen de publiek toegankelijke informatie die organisaties beschikbaar stellen. Daaruit kan worden geconcludeerd in welke mate er, op basis van de in het theoretisch kader bepaalde factoren, sprake is van een grondige implementatie van de GDPR.

In het theoretisch kader wordt allereerst institutionele theorie worden bekeken om richting te geven aan het vervolg van het literatuuronderzoek. Het onderscheid tussen de private en de publieke sector wordt daarin behandeld en er zal worden vastgesteld welke factoren bepalend zijn voor de grondigheid van GDPR-implementaties. Ook zal gezocht worden naar bronnen die meer informatie bieden over privacy(wetgeving) en de wijze waarop dergelijke wetgevingen/verordeningen worden geïmplementeerd.

Vervolgens zal nagegaan worden aan welke maatregelen voldaan moet worden om te voldoen aan de GDPR. Deze maatregelen zullen leiden tot factoren die beoordeeld zullen worden in dit onderzoek. Hierover worden aan het eind van het theoretisch kader hypotheses opgesteld.

In de methodologie worden het conceptueel ontwerp en het technisch model van het onderzoek uitgewerkt. Het onderzoek wordt vervolgens op basis van het technisch ontwerp uitgevoerd. De resultaten uit de analyse geven daarop een beeld van de mate van grondigheid waarmee de GDPR-maatregelen zijn geïmplementeerd. In deze analyse wordt gekeken wat de verschillen zijn tussen de publieke en private sector.

In de discussie, conclusies en aanbevelingen worden de resultaten verder geduid en wordt aangegeven in hoeverre deze vergelijkbaar zijn met resultaten van eerder onderzoek en wat dit onderzoek aan kennis heeft toegevoegd. Ook wordt hierin besproken wat is opgevallen, wat hier mogelijke verklaringen voor zijn en wat de aanbevelingen zijn voor vervolgonderzoek.

2. Theoretisch kader

2.1. Onderzoeksaanpak

Om tot een antwoord te komen op de hoofd- en subvragen uit de opdrachtformulering, wordt in dit hoofdstuk een theoretisch kader geschetst voor dit onderzoek. Daarin worden de onderzoeksvragen gekoppeld aan bestaand theoretisch onderzoek en worden hypotheses opgesteld aan de hand van één of meerdere wetenschappelijke theorieën. Hiervan is het doel om een overzicht te verkrijgen van de beschikbare en ontbrekende kennis en de gangbare theorieën over de onderwerpen van dit onderzoek.

Ook wordt er gekeken naar de wijze waarop bronnen en zoektermen worden gekozen en hoe de relevantie van gevonden literatuur wordt bepaald, dit is terug te vinden in Appendix 1.

2.1.1. Doel van theoretisch kader

Uit de hoofd- en deelvragen die zijn opgesteld bij de opdrachtformulering van de inleiding (1.4) zijn een aantal hoofdonderwerpen te halen. Dat zijn *onderscheid publiek en private sector, symbolisch versus grondig*, *privacy(wetgeving)* en *maatregelen en factoren GDPR*.

In het onderwerp *'Onderscheid publieke en private sector'* wordt kennis opgedaan over institutionele theorie (DiMaggio & Powell, 1983), eerder onderzoek en de wijze waarop organisaties in dit

onderzoek worden ingedeeld. Bij het onderwerp *'symbolisch versus grondig'* wordt eerder onderzoek met deze opzet geanalyseerd. Dit geeft een beeld van de wijze waarop er in eerder onderzoek is omgegaan met de vraagstukken waarbij implementaties geclassificeerd worden als symbolisch of grondig.

Daarna wordt voor het onderwerp *'Privacy(wetgeving)'* onderzocht welke ontwikkelingen er de afgelopen jaren hebben plaatsgevonden en wat er aan wetenschappelijke literatuur beschikbaar is over de implementatie van soortgelijke wetgeving. Bij *'Maatregelen en factoren GDPR'* wordt ten slotte geanalyseerd welke maatregelen organisaties moeten nemen om te voldoen aan de GDPR en welke factoren daarvan bruikbaar zijn voor dit onderzoek.

Met dit theoretisch kader ontstaat een beeld van welke kennis over dit onderwerp beschikbaar is en welke toevoeging dit onderzoek heeft op deze bestaande kennis. Hieruit volgen een onderzoeksmodel en hypotheses, die als basis dienen voor het bespreken van de verwachtingen en conclusies van dit onderzoek.

2.2. Uitvoering

In de uitvoering van het zoeken van bronnen, lag de focus op de verdeling van onderwerpen zoals in het doel van het theoretisch kader (2.1.1) beschreven. Bij het zoeken bleek dat er geen papers te vinden zijn die over precies hetzelfde onderwerp als dit onderzoek gaan. Wel zijn er papers die een overlap hebben van meerdere hoofdonderwerpen (zie Appendix 1, Figuur 1). Voor de onderwerpen afzonderlijk waren er in alle gevallen papers te vinden. Een deel daarvan is aangedragen bij aanvang van dit onderzoekstraject, zoals de onderzoeken geciteerd bij de onderwerpen *symbolisch versus grondig* en *privacy(wetgeving)* en een tweetal onderzoeken dat zowel de implementatie van privacywetgeving beschrijft, als een onderscheid maakt tussen de publieke en private sector.

De andere resultaten zijn gevonden door de eerdergenoemde online databases te benutten met (combinaties van) de vastgestelde zoektermen (zie Appendix 1, Zoektermen). Twee uitzonderingen daarop zijn achterliggende theorieën, voor zowel de stakeholder theorie als de institutionele theorie is backward snowballing toegepast. Van forward snowballing is geen gebruik gemaakt.

Voor papers die specifiek over de GDPR gaan is minder waarde gehecht aan het aantal keer dat de papers zijn geciteerd, omdat dit vaak zeer recente artikelen betreft. Papers over de GDPR betreffen tot nu toe enkel informatie die voornamelijk gericht is op de aanloop naar de invoering van de GDPR. Over de implementatie van de GDPR is op het moment van het literatuuronderzoek nog geen onderzoek beschikbaar.

De nieuwsbronnen zijn voornamelijk in het Nederlands gezocht. Gezien de berichten over publieke organisaties die moeite hebben met de implementatie (de Vries, Joost & Sys, Myra, 2019; Hofmans, Tijs, 2019) en dat de Autoriteit Persoonsgegevens onvoldoende capaciteit heeft om breed te controleren op naleving van de GDPR (Mebius, Dion, 2018), zal de focus van dit onderzoek ook bestaan uit Nederlandse en in Nederland opererende organisaties. De resterende gevonden literatuur is Engelstalig. In dit onderzoek worden in totaal vier nieuwsberichten, twee rapporten en twaalf papers geciteerd.

2.3. Resultaten en conclusies

De resultaten worden weergegeven op basis van de onderwerpen zoals deze in het doel van het theoretisch kader (2.1.1) staan beschreven.

2.3.1. Onderscheid publieke en private sector

De onafhankelijke variabele is in dit onderzoek de sector (privaat, publiek of semipubliek) van de onderzochte organisaties. Daarmee is het van belang om te begrijpen hoe de sector van een organisatie invloed heeft op afhankelijke variabelen. Dat wordt voor dit onderzoek gedaan aan de hand van institutionele theorie en gerelateerd onderzoek.

Institutionele theorie

In dit onderzoek is het voornaamste uitgangspunt de institutionele theorie, waarbij organisaties die zich binnen eenzelfde 'instituut' bevinden de neiging vertonen in structuur, processen en standaarden op elkaar te gaan lijken (DiMaggio, Paul J. & Powell, Walter W., 1983). Door in deze studie onderscheid te maken tussen de sectoren *publiek*, *semipubliek* en *privaat*, is de verwachting dat er patronen ontstaan binnen deze sectoren die toe te kennen zijn aan deze institutionele theorie.

De drie redenen van gelijkenissen tussen organisaties die in institutionele theorie worden beschreven zijn:

1) Coercive (gedwongen), bijvoorbeeld door wetgeving of accreditatiestandaarden;
2) Normative (normatief), waarbij compliance aan geldende normen aan de hand externe verwachtingen wordt aangemoedigd;
3) Mimetic (nadoen), zoals door het volgen van industrieleiders in werkwijzen of focus.

In het kader van dit onderzoek scheppen deze redenen een aantal verwachtingen over de resultaten die behaald worden. Per reden zou dat de volgende implicaties kunnen hebben:

Coercive:

De Autoriteit Persoonsgegevens heeft aangegeven dat de eerste jaren dat de GDPR van kracht is een striktere handhaving geldt voor de publieke sector (Mebius, 2018). De wetgeving is voor alle sectoren gelijk. Maar deze intensievere handhaving voor de publieke sector, wordt deze sector gedwongen om te voldoen aan een grondige implementatie van de GDPR. Dat wekt voor de resultaten van dit onderzoek de verwachting dat er een hogere score voor grondigheid wordt behaald door de publieke sector dan door de private sector.

Normative:

De Autoriteit Persoonsgegevens heeft de focus voor de eerste jaren dat de GDPR van kracht is voornamelijk gericht op organisaties waarbij veel met persoonsgegevens wordt gewerkt. De overheid wordt daarbij als voorbeeld genoemd. Ook heeft de overheid wat betreft het naleven van wetgeving een voorbeeldfunctie te vervullen (Mebius, 2018). Gezien de verwachtingen dat de overheid vanuit een voorbeeldfunctie handelt, brengt dat onder het kopje 'normative' de verwachting dat organisaties vanuit de publieke sector hoger op grondigheid van GDPR-implementatie scoren.

Daarnaast zijn er van andere organisaties die veel persoonsgegevens verwerken verwachtingen over de mate waarin ze aan de GDPR voldoen, denk daarbij aan zorginstellingen en organisaties die in data handelen. De mate waarin organisaties persoonsgegevens verwerken of verhandelen wordt in dit onderzoek echter niet meegenomen. Daarom zal hierin geen onderscheid worden gemaakt in de resultaten.

Mimetic:

> Het is voorafgaand aan het verzamelen van data lastig te voorspellen op welke wijze mimetic een rol speelt voor de organisaties in dit onderzoek. Daarmee is het niet duidelijk wat er te verwachten valt in dit opzicht. Wat er vanuit dit punt wel zal worden meegenomen, is dat er gelet wordt op patronen in hoe gegevens worden gedeeld. Dit hangt mogelijk samen met hoe de Autoriteit Persoonsgegevens over de GDPR communiceert, al is dat geen onderwerp van dit onderzoek.
>
> Hieruit is mogelijk af te leiden dat organisaties binnen sectoren de wijze van communicatie over de GDPR, in bijvoorbeeld privacyverklaringen en jaarverslagen, van elkaar hebben overgenomen. Dat kan ertoe leiden dat de score voor een bepaalde sector hoger of lager uitvalt, afhankelijk van de kwaliteit van de overgenomen informatieverstrekking.

De verwachting van dit onderzoek is dat er tussen de sectoren verschillen zitten in hoe zij hun implementatie van de GDPR hebben uitgevoerd. Met behulp van institutionele theorie wordt er in de resultaten gereflecteerd op wat de gevonden overeenkomsten binnen sectoren zijn en hoe verschillen in scores voor grondigheid te duiden zijn.

Gerelateerd onderzoek

In een Maleisisch onderzoek over compliance aan nieuwe privacywetgeving, de Personal Data Protection Act (PDPA), werd geconcludeerd dat organisaties uit de private sector in Maleisië significant hoger scoren op compliance dan organisaties uit de publieke sector (Chua, Herbland, Wong, & Chang, 2017). Dit onderzoek werd uitgevoerd op basis van een analyse op het privacybeleid van organisaties. In dit deel van het onderzoek zijn de scores over 152 organisaties vergeleken. Volgens de onderzoekers was deze uitkomst deels te wijten aan de gebruikte standaardtemplates voor privacybeleid bij de overheid.

Verder kan er gekeken worden naar de reputatie van de publieke sector, waarbij het voornaamste onderscheid te maken is tussen organisaties in de publieke sector die worden gezien als bureaucratisch (organisaties met wetgevende en autoritaire functies) en flexibel (onderzoek en semi-commerciële functies) (Luoma-aho, 2008). Gezien deze verschillen in reputatie kan het onderscheid in compliance aan privacywetgeving mogelijk gekoppeld worden aan het soort publieke organisatie dat wordt onderzocht. Het meenemen van de semipublieke sector, die in bovenstaand onderzoek onder de ‘semi-commerciële’-functies zou vallen, zou daarmee wellicht kunnen aantonen dat de verhoogde flexibiliteit die deze organisaties aan reputatie genieten van invloed is op een meer grondige GDPR-implementatie.

Ten slotte is, in een ‘State of the Art’-onderzoek uit 2012, gekeken naar verschillen in gedrag tussen medewerkers van de publieke en de private sector. Hieruit blijkt dat er hoewel er verschillen worden gemeten in bijna alle aspecten waarop onderzoek is gedaan, er geen duidelijke lijn in de uitkomsten te vinden is (Baarspul & Wilderom, 2012, Volume 13, Uitgave 7). Omdat onderzoek veelal tegenstrijdige resultaten geeft, valt hieruit niet op te maken welke resultaten er voor dit onderzoek te verwachten vallen. Wel geeft het aan dat het onderwerp interessant is omdat er nog geen eenduidige voorspelling te maken is over welke resultaten dit onderzoek zal opleveren.

Organisaties

Hoe het onderscheid tussen de private, semipublieke en publieke sector wordt gemaakt in dit onderzoek zal worden bepaald op basis van de definitie die het Centraal Bureau voor de Statistiek

(CBS) aanhoudt. In het rapport 'Wat rekent het CBS tot de sector Overheid' (Centraal Bureau voor de Statistiek, 2018) wordt aangegeven dat de termen 'publieke sector' en 'private sector' geen standaardbetekenis hebben. Door het CBS wordt dit onderscheid gemaakt door middel van 'controle door overheid' en 'markt/niet markt'. Het CBS kijkt verder naar een splitsing tussen de centrale overheid en de lokale overheid. Deze vallen in dit onderzoek samen onder de noemer 'publieke sector'. Hoe de organisaties in dit onderzoek worden gekozen staat omschreven in de methodologie (3.2.1) en Appendix 2.

2.3.2. Symbolisch versus grondig

In dit onderzoek worden scores voor de grondigheid van GDPR-implementaties gemeten, die vervolgens kunnen worden gezien op een schaal van een volledig symbolische implementatie tot een grondige implementatie. De opzet van dit onderzoek is daarmee in de vorm van symbolisch versus grondig. In eerder onderzoek is gebleken dat de wijze waarop beleid is toegepast tussen de classificaties symbolisch en grondig ingeschaald kan worden (Christmann & Taylor, 2006). Alhoewel alle organisaties moeten voldoen aan de wetgeving van de GDPR, zit er in de praktijk een groot verschil in de grondigheid waarmee de GDPR is geïmplementeerd. De wijze waarmee een implementatie beoordeeld wordt zit daarmee in een spectrum van symbolisch tot grondig, om zo een idee te geven in hoeverre een organisatie aan de vereiste maatregelen heeft voldaan.

Daarbij moet dus verder gekeken worden dan alleen het opstellen van beleid, omdat de handeling van het opstellen van beleid los gezien kan worden van de daadwerkelijke implementatie volgens Christmann & Taylor (2006). In dit onderzoek verschilt de wijze waarop de mate van grondigheid bepaald wordt, omdat de score op basis van publiek beschikbare bronnen bepaald wordt. Door de maatregelen en factoren van de GDPR (2.3.4) te benoemen, kan aan de hand daarvan onderzocht worden welke van deze factoren vanuit openbare bronnen terug te zien zijn. Door dit op een aantal maatregelen en daarbij behorende factoren toe te passen, geeft de score per organisatie en sector aan of de implementatie als symbolisch of grondig kan worden classificeert.

2.3.3. Privacy(wetgeving)

Volgens de 'State of the Information Privacy Literature' (Pavlou, 2011) liggen volgens de wetenschappelijke literatuur een aantal zorgen over information privacy bij consumentenbescherming. De eerste zorg daarvan is het oneigenlijk gebruik van persoonsgegevens, met als gevolg nadelige effecten als ongevraagde post, creditcardfraude en identiteitsdiefstal. De tweede zorg gaat over het gebruik van persoonsgegevens voor andere doeleinden dan aangegeven bij de oorspronkelijke uitwisseling van data. Zoals het delen van data met derden en het ongeautoriseerd hergebruiken van persoonlijke informatie.

Daar staat tegenover dat er voordelen aan het gebruik van persoonsgegevens zitten, zoals financiële beloningen, personalisatie en de mogelijkheden die social media aan gebruikers biedt. Persoonsgegevens worden daarbij door velen als economische ruil gezien, waarbij de risico's van het delen van persoonsgegevens worden afgewogen tegen de genoemde voordelen. In het State of Information Privacy onderzoek wordt er voornamelijk gefocust op het niveau van het individu. Over andere niveaus (groep, organisatie, maatschappij) is minder literatuur beschikbaar en liggen er kansen voor vervolgonderzoek.

Nadat het hierboven benoemde 'state of the information privacy'-onderzoek is uitgekomen, is er veel gebeurd op het gebied van privacy en gegevensbescherming. Denk daarbij aan een veranderde kijk op privacy, onder meer na onthullingen van Edward Snowden, waardoor in plaats van organisaties juist privacy voorstanders meer invloed hebben gekregen op de vorming van de GDPR

(Rossi, 2018). De GDPR is echter geen resultaat van deze ontwikkelingen, aangezien de GDPR grotendeels gebaseerd is op het uniformeren van bestaande privacywetgeving die in de Europese Unie eerder per lidstaat was geregeld (Tikkinen-Piri, Rohunen, & Markkula, 2018).

Implementatie

Uit eerder onderzoek blijkt dat voldoen aan bestaande privacywetgeving niet vanzelfsprekend is. Zo kwam in een Israëlisch onderzoek waarin de wet, privacybeleid en dataverzameling van websites naast elkaar werden gelegd, naar voren dat slechts een klein deel van de onderzochte websites voldeed aan juridische vereisten (Birnhack & Elkin-Koren, 2010). Los van het lage percentage van websites dat voldeed aan de wet, tussen de 16 en 22 procent, valt het verschil in compliance tussen grotere en kleinere organisaties op. Waarbij grotere organisaties over het algemeen beter voldoen aan wetgeving dan kleinere organisaties. Dat verschil is ook interessant voor dit onderzoek, omdat grotere organisaties ook wat betreft GDPR meer juridische en financiële middelen hebben om aan de voorwaarden te voldoen.

Ander onderzoek geeft inzicht over de implementatie van privacywetgeving naar aanleiding van de invoering van de Personal Data Protection Act (PDPA) in 2010 in Maleisië. Daaruit blijkt dat ondanks verschillen in score voor compliance, veel van de ruim driehonderd organisaties niet voldoen aan de voorwaarden van de PDPA (Chua, Hui Na, Herbland, Anthony, Wong, Siew Fan, & Chang, Younghoon, 2017). Resultaten tonen dat organisaties uit de private sector hoger scoren op compliance dan organisaties uit de publieke sector. De onderzoekers geven daarover aan dat dit een interessante bevinding is, omdat overheidsorganisaties bij uitstek het goede voorbeeld zouden moeten geven wat betreft het naleven van wetgeving. Toch kwam dit niet uit het onderzoek naar voren. Met als mogelijke verklaring een korter privacybeleid bij de onderzochte overheidsorganisaties.

De content analyse in dit onderzoek draait beperkt om woordaantallen voor de factoren van de jaarverslagen (zie 3.2.3 en Appendix 3). Daarom is in dit onderzoek niet de verwachting dat de publieke sector lager scoort op hun implementatie dan de private sector. Het is daarnaast mogelijk dat er contextuele verschillen zijn waardoor organisaties in Maleisië en de Europese Unie verschillend met nieuwe privacywetgeving omgaan, waardoor het bij een verschil in uitkomsten interessant kan zijn om de verschillen in de context van deze onderzoeken te analyseren.

2.3.4. Maatregelen en factoren GDPR

Het is in dit onderzoek van belang om te weten welke maatregelen er voor de GDPR genomen moeten worden door organisaties. Op basis van deze maatregelen is het mogelijk de grondigheid van GDPR-implementaties te bepalen. Eén van de te voorziene moeilijkheden daarin is dat de GDPR niet exact voorschrijft hoe de wetgeving geïmplementeerd dient te worden. Wel wordt verwacht dat organisaties interne maatregelen moeten nemen om aan de principes van databescherming volgens de GDPR te voldoen (Tankard, 2016).

Er is ook een aantal nieuwe maatregelen dat met de GDPR is geïntroduceerd. Een onderzoek naar de GDPR-artikelen en de daarbij behorende maatregelen en implicaties (Tikkinen-Piri, Christina, Rohunen, Anna, & Markkula, Jouni, 2018), geeft een overzicht op welke wijze de GDPR impact heeft op organisaties en hun data- en privacybeleid. Van de maatregelen die staan beschreven, kan de volgende selectie gemaakt worden van maatregelen die vanuit publieke bronnen te controleren zijn.

Een aantal van de maatregelen voor de GDPR waarop dit onderzoek verder gebaseerd zal worden is:

- Het verstrekken van transparante en begrijpelijke informatie over de verwerking van persoonsgegevens;

- Het privacybeleid is gemakkelijk te vinden op de website van de organisatie en is in begrijpelijke taal geschreven;
- Het verstrekken van procedures en voorwaarden waarop betrokkenen hun rechten kunnen uitoefenen;
- Organisaties en hun personeel zijn zich bewust van het belang en de verplichtingen over privacy.

Deze maatregelen zijn grotendeels in te delen in 'transparantie' en 'bewustzijn'. Zo liggen maatregelen niet alleen op het hebben van processen met betrekking tot informatieverwerking, maar ook op het communiceren hierover. Datzelfde geldt ook voor het verstrekken van informatie over hoe betrokkenen hun rechten kunnen uitoefenen. Daarnaast gaat een deel van de maatregelen uit van het privacybewust maken van organisaties en hun medewerkers. Zoals het verhogen van privacybewustzijn op organisatieniveau en de daarbij behorende trainingen bij de implementatie van de GDPR (Tikkinen-Piri, Christina, Rohunen, Anna et al., 2018). Het verhogen van privacybewustzijn is in de praktijk te meten door een aanpak zoals in het Maleisische onderzoek (Chua, Herbland, Wong, & Chang, 2017) te volgen, waar het aantal (tref)woorden wordt gemeten en op basis daarvan een score wordt toegekend. De mate waarin een organisatie communiceert over privacy en de GDPR, en de verandering hierin ten opzichte van vóór de GDPR van kracht ging, kan worden meegenomen om de grondigheid van de GDPR-implementatie te bepalen.

Daarnaast is er vanuit de Autoriteit Persoonsgegevens een lijst met rechten gedeeld, waaraan organisaties aan moeten voldoen sinds de GDPR van kracht is (Autoriteit Persoonsgegevens, Privacyrechten, sd). Daarin staan de rechten waarover transparant gecommuniceerd moet worden in de privacyverklaringen van organisaties. Dat zijn 'Recht op informatie', 'Recht op inzage', 'Recht op rectificatie', 'Recht op vergetelheid', 'Recht op dataportabiliteit', 'Recht van bezwaar', 'Recht op beperking van gegevensverwerking' en de mogelijkheid om een klacht te melden bij de Autoriteit Persoonsgegevens.

Deze maatregelen waren niet of in mindere mate van kracht voor de GDPR, waarmee controle hierop een indicatie geeft van de grondigheid waarmee de GDPR is geïmplementeerd. De exacte factoren en de bijbehorende protocollen zijn verder uitgewerkt in 3.2.3 en Appendix 3.

2.4. Doel van het vervolgonderzoek

De resultaten en conclusies uit het theoretisch kader wekken de verwachting dat er een verschil meetbaar zal zijn in de grondigheid waarmee de publieke sector en de private sector de GDPR hebben geïmplementeerd. Wat dat verschil zal zijn, is gezien de literatuur nog niet vast te stellen, omdat uitkomsten uit eerder onderzoek niet consistent zijn en niet helder verklaard worden, naast het bestaan van mogelijke culturele verschillen tussen Nederland (en de EU) en de plaatsen waar eerder onderzoek heeft plaatsgevonden (Zoals de Verenigde Staten, Israël en Maleisië).

Verder is er een verschil te verwachten tussen de wijze waarop grote en kleine organisaties GDPR-maatregelen doorvoeren. Door het verschil in grootte van organisaties op zowel de publieke en private sector te onderzoeken, wordt ontdekt of deze factor een bepalende rol speelt voor GDPR-implementaties. Vanuit het theoretisch kader is hier een grotere mate van grondigheid te verwachten bij grote organisaties dan bij kleine organisaties.

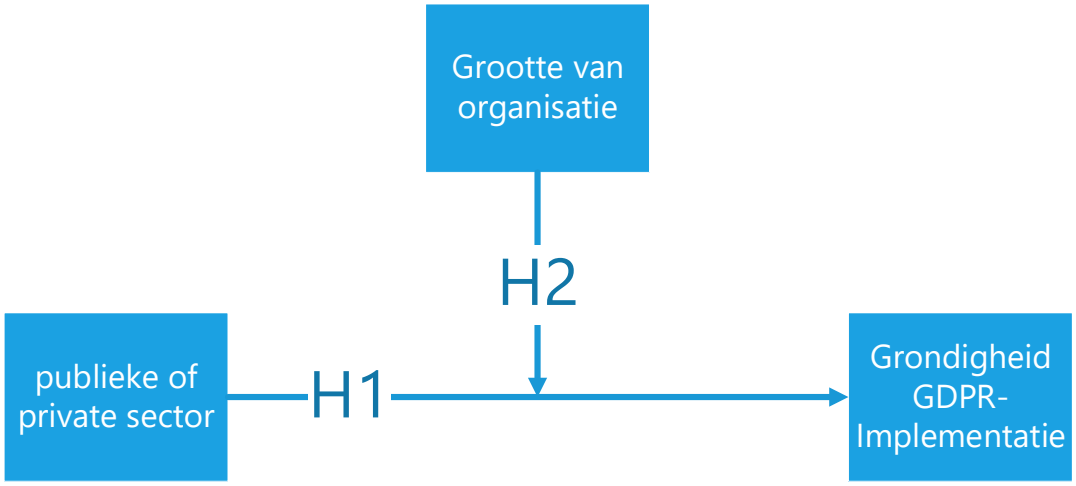
2.4.1. Onderzoeksmodel

Dit onderzoek richt zich op de invloed van de sector waarin een organisatie zich bevindt op de mate van grondigheid waarmee de GDPR is geïmplementeerd, of wel de implementatiestrategie. Daarnaast zal de grootte van de organisatie worden meegenomen als mediërende variabele.

Bij de sector wordt een onderscheid gemaakt tussen organisaties uit de publieke, semipublieke en private sector. De grootte van een organisatie wordt bepaald op basis van de hoeveelheid medewerkers van de organisatie (zie Appendix 2).

De implementatiestrategie wordt gezien als de mate van grondigheid waarmee de GDPR is geïmplementeerd. GDPR-maatregelen worden hiervoor omgezet in een aantal meetbare factoren, waaraan een organisatie wel of niet kan voldoen. Of zijn per factor wel of niet voldoen, leidt tot een score die in dit onderzoek de grondigheid weergeeft (zie Appendix 3).

Dit leidt tot het onderzoeksmodel zoals te zien in Figuur 1.



Figuur 1 Onderzoeksmodel

2.4.2. Hypotheses

H1a
Organisaties die vallen binnen de publieke sector, scoren hoger op grondigheid van GDPR-implementatie.
H1b
De score voor grondigheid van GDPR-implementatie van de semipublieke sector valt tussen de score van de publieke en de score van de private sector in.

H2
Het effect dat de sector heeft op de score van grondigheid van GDPR-implementatie, wordt beïnvloed door de organisatiegrootte.

3. Methodologie

3.1. Conceptueel ontwerp: keuze van onderzoeksmethode(n)

Dit onderzoek betreft een kwantitatief onderzoek, dat wil zeggen dan er gekwantificeerde data wordt verzameld en geanalyseerd om tot een antwoord op de onderzoeksvragen te komen (Saunders, Lewis, & Adrian, 2016). Er is om een aantal redenen de voorkeur gegeven aan een kwantitatief onderzoek in plaats van een kwalitatief onderzoek. De voornaamste redenen daarvan zijn de schaal en de aard van het onderzoek.

Kwantitatief onderzoek beter werkt op grotere schaal, wat benodigd is om een verschil in grondigheid van GDPR-implementatie tussen de publieke en private sector te meten en op te merken. Met kwalitatieve methoden zou dat een hoeveelheid tijd kosten, die voor dit onderzoek

niet in die mate beschikbaar is. De aard van het onderzoek draait meer om het vinden van een trend, dan om het verklaren daarvan. Daarvoor is kwantitatief onderzoek meer geschikt. De uitkomsten kunnen mogelijk uitvoerig verklaard worden in een opvolgend kwalitatief onderzoek, maar dat valt buiten de scope van dit onderzoek.

Binnen de scope van dit onderzoek zullen de voornaamste uitkomsten de conclusies zijn over de invloed van het behoren tot de publieke of de private sector én van de grootte van de organisatie, op de grondigheid waarmee organisaties de GDPR hebben geïmplementeerd.

Waar in eerdere hoofdstukken de probleemstelling, het theoretisch kader en het onderzoeksmodel zijn uitgewerkt, volgt in dit conceptueel ontwerp van het onderzoek de aanpak om de benodigde gegevens te verzamelen, te classificeren en te analyseren.

Het verzamelen van de gegevens gebeurt door middel van de volgende stappen:

1) Bepalen hoeveel en welke organisaties onderzocht worden;
2) Het indelen van deze organisaties in de drie groepen van de verklarende variabele (publieke sector, semipublieke sector en private sector);
3) Grootte van de organisaties bepalen;
4) Factoren uitwerken die indicatief zijn voor een grondige implementatie van de GDPR;
5) Gegevens verzamelen over de gekozen factoren;
6) Uitvoeren van een statistische analyse;
7) Trekken van conclusies.

De eerste drie punten gaan over de organisatiekeuze. Deze keuze wordt gemaakt op basis van de in het theoretisch kader omschreven definitie van sectoren (zie 3.2.1). De hoeveelheid, verdeling en groottebepaling van organisaties is uitgewerkt in Appendix 2.

Voor de factoren is gekozen de classificatie toe te passen op basis van de best aansluitende methode. Allereerst wordt een onderscheid gemaakt tussen factoren met betrekking tot privacy statements en factoren die van toepassing zijn op jaarverslagen. Voor de factoren bij privacy statements zal content geanalyseerd worden op beschikbaarheid van informatie, waarbij wordt gezocht naar beschikbare kwalitatieve informatie die wordt gecategoriseerd op een wijze die kwantitatief verwerkbaar is (Saunders, Lewis, & Adrian, 2016).

Voor maatregelen die niet binair te meten zijn, worden criteria benoemd die een score vertegenwoordigen. Dat zal in veel gevallen een drempelwaarde van een aantal (tref)woorden of een percentage zijn. De factoren en hun protocollen staan verder omschreven in Appendix 3.

Vervolgens zal met deze gegevens door middel van een multivariate regressieanalyse het soort organisatie en de grootte worden geanalyseerd, aan de hand van de score die behaald is bij de factoren die de grondigheid van de GDPR-implementatie vertegenwoordigd.

De scope van dit onderzoek beperkt zich tot gegevens die vanuit publieke bronnen beschikbaar zijn. Dit zijn voornamelijk privacyverklaringen, jaarverslagen en organisatiewebsites. Dat stelt dit onderzoek in staat om in korte tijd een groot aantal organisaties te onderzoeken. Dit betekent tegelijkertijd dat de classificaties niet op een kwalitatieve wijze worden gevalideerd. Vervolgonderzoek op kwalitatief vlak waarmee resultaten gevalideerd worden is daarvoor wenselijk.

3.2. Technisch ontwerp: uitwerking van de methode

In het technisch ontwerp wordt de praktische uitvoering van het conceptuele ontwerp beschreven.

3.2.1. Organisaties

Dat begint bij het bepalen hoeveel organisaties zullen worden meegenomen in het onderzoek. Dit is een afweging tussen het verkrijgen van zoveel mogelijk data en de haalbaarheid. Een grote dataset komt ten gunste aan de betrouwbaarheid van het onderzoeksresultaat, maar gezien de beperkte scope en tijd voor dit onderzoek is ook haalbaarheid een factor. Gezien de periode die voor dit onderzoek is ingepland, is als doel een dataset van tussen de 100 en 150 organisaties te verzamelen.

Hoe die organisaties worden geselecteerd is op basis van het onderscheid tussen overheid, semioverheid en private sector, zoals in 2.3.1 en Appendix 2 is omschreven. Voor de selectie van organisaties kan voor de (semi)publieke sector gebruik gemaakt worden van het register dat te vinden is op de website van de overheid (Almanak Overheid, sd). Voor de private sector wordt er een selectie gemaakt van beursgenoteerde organisaties, gezien de publieke toegang tot informatie. Het voornaamste onderscheid in het onderzoek bestaat uit de publieke en de private sector. De tussenvorm van beide, de semipublieke sector, speelt een kleinere rol. Daarom wordt gestreefd naar een verdeling van grofweg veertig procent overheidsinstellingen, veertig procent private sectorinstellingen en twintig procent semioverheidsinstellingen gestreefd.

Gezien de organisaties op basis van het onderscheid tussen (semi)publieke en private sector worden geselecteerd, is met het bepalen welke organisaties worden onderzocht direct de bepaling van de verklarende variabele in het onderzoek bekend. Vervolgens wordt de grootte van de organisatie bepaald op basis van het aantal werknemers. Gezien de haalbaarheid van het onderzoek is gekozen voor twee groepen in deze categorie. Deze groepen staan relatief ten opzichte van elkaar en worden ‘Klein’ genoemd voor organisaties met 1700 of minder werknemers, en ‘Groot’ voor alle organisaties met meer dan 1700 werknemers. Er wordt bij grootte niet naar andere soorten grootte gekeken, zoals bijvoorbeeld winst of jaaromzet, omdat deze gegevens voor de (semi)publieke sector een minder relevant zijn.

3.2.2. Bronnen

Dit onderzoek is gebaseerd op het verkrijgen van gegevens uit publieke bronnen. Dat maakt dat de resultaten van dit onderzoek afhangen van informatie die organisaties publiekelijk beschikbaar maken. Daarmee zijn de uitkomsten, zeker per organisatie gezien, deels afhankelijk van de wijze waarop organisaties communiceren over privacy en de GDPR. Het gebruik maken van publieke bronnen maakt dat er meer organisaties kunnen worden onderzocht, wat ten gunste komt van de validiteit van het onderzoek.

Er wordt per organisatie gebruik gemaakt van de volgende bronnen:

- De organisatiewebsite;
- De privacyverklaring van de organisatie;
- Jaarverslagen (van 2017 en 2018);

Deze bronnen worden geraadpleegd om informatie te vinden over de onafhankelijke variabelen van dit onderzoek en de hieronder beschreven factoren.

3.2.3. Factoren en maatregelen GDPR

De factoren voor dit onderzoek worden verdeeld in twee groepen:

- Tien factoren met betrekking tot de privacyverklaring;
- Vijf factoren met betrekking tot het jaarverslag.

Er ligt meer focus op de factoren voor de privacyverklaringen om dat deze duidelijker meetbaar zijn en de interpretatie minder subjectief is dan die voor de jaarverslagen. De factoren van de privacyverklaringen gaan om de beschikbaarheid van informatie en transparantie over privacyrechten van betrokkenen. Waar de factoren in de jaarverslagen voornamelijk draaien om communicatie over privacy en de GDPR en daarmee het privacybewustzijn van de organisatie. Deze factoren zijn gekozen op basis van de in het theoretisch kader genoemde rechten en maatregelen (zie 2.3.4).

Voor de privacyverklaring zijn de volgende factoren gekozen:

- Factor 1.1: Aanwezigheid privacy statement
- Factor 1.2: Recht op informatie
- Factor 1.3: Recht op inzage
- Factor 1.4: Recht op dataportabiliteit
- Factor 1.5: Recht op rectificatie
- Factor 1.6: Recht van bezwaar
- Factor 1.7: Recht op beperking van gegevensverwerking
- Factor 1.8: Recht op vergetelheid
- Factor 1.9: Mogelijkheid klacht Autoriteit Persoonsgegevens
- Factor 1.10: Verwijzing naar privacyverklaring op homepage

De factoren voor de jaarverslagen zijn als volgt:

- Factor 2.1: Aantal woorden in jaarverslag besteed aan privacy
- Factor 2.2: Percentage jaarverslag besteed aan privacy
- Factor 2.3: Aantal hits op privacy/GDPR-trefwoorden in jaarverslag
- Factor 2.4: Ontwikkeling aantal trefwoorden ten opzichte van vorig jaar
- Factor 2.5: Verwijzing naar privacy statement in jaarverslag

Voor elk van deze factoren waaraan wordt voldaan wordt één punt behaald, bij niet voldoen wordt er geen punt behaald. Het protocol voor meten en beoordelen van deze factoren staat omschreven in Appendix 3. Er valt per organisatie een score te behalen tussen de nul en vijftien punten. Waarbij de score de mate van grondigheid van GDPR-implementatie aangeeft. Deze score wordt bijgehouden en gebruikt voor de statistische analyse van de resultaten (zie 4.1.1).

3.3. Gegevensanalyse

De hoofdanalyse van de onderzoeksdata zal een multivariate regressieanalyse zijn. Met deze analyse worden algemene trends en de spreiding van de data omschreven (Saunders, Lewis, & Adrian, 2016). Het doel van de analyse is om aan de hand van de verzamelde gegevens de relevante en significante uitkomsten te vinden die helpen om de onderzoeksvragen (zie 1.4) te beantwoorden.

Hiervoor worden eerst een aantal andere analyses uitgevoerd. Allereerst beschrijvende statistiek, waarin de verzamelde data globaal geanalyseerd wordt op onder meer aantallen en gemiddelden.

Vervolgens wordt er de One Way ANOVA (F-test) uitgevoerd om na te gaan of de variantie tussen de verschillende categorieën significant verschilt. En waar nodig wordt dit doorgezet in specifiekere Independent sample T-tests, waarin ook waarden binnen factoren ten opzichte van elkaar worden vergeleken.

Daarnaast wordt er analyse op de bivariate correlaties uitgevoerd, om de samenhang van onderzochte factoren te analyseren. Waarna er een multivariate regressieanalyse plaatsvindt en het modererend effect wordt berekend.

3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

Het is belangrijk om te benadrukken wat er voor dit onderzoek wel en niet wordt onderzocht. Gezien de keuze om voor dit onderzoek publieke bronnen te gebruiken, is de validiteit ook gebaseerd op de kwaliteit en beschikbaarheid van de publiek verkrijgbare informatie.

Het doel van het onderzoek is om een conclusie te trekken over verschillen in GDPR-implementatie van een groep organisaties, niet om tot conclusies over individuele organisaties te komen. Voor een realistische inschatting voor individuele organisaties is kwalitatief onderzoek beter geschikt.

Daarnaast moeten resultaten van dit onderzoek gezien worden als momentopname. De informatie waarop resultaten en conclusies gebaseerd worden is veranderlijk, waardoor ook het moment van meten invloed kan hebben op de uitkomst. Er wordt gestreefd de periode waarin de data verzameld wordt beperkt te houden, zodat organisaties over eenzelfde periode beoordeeld worden. Dat heeft als consequentie dat eventuele veranderde of nieuwe informatie niet wordt meegenomen in dit onderzoek.

3.4.1. Validiteit

Wat betreft validiteit wordt er een onderscheid gemaakt tussen interne en externe validiteit (Saunders, Lewis, & Adrian, 2016). Bij interne validiteit wordt bepaald of er met de gekozen onderzoeksmethode de juiste conclusies getrokken kunnen worden. De externe validiteit zegt iets over de mate waarin de conclusies te generaliseren naar een bredere context dan de groep onderzochte organisaties.

De interne validiteit wordt geborgd door vanuit de literatuur factoren vast te stellen die indicatief zijn voor een grondige implementatie. Door te zoeken naar meerdere van deze maatregelen, kan er op basis van een score een conclusie getrokken worden over de grondigheid van de GDPR-implementatie. Een evenwichtige keuze in de te onderzoeken maatregelen met transparante criteria en argumentatie, is voor de scope van dit onderzoek voldoende om aan de eisen voor de interne validiteit te voldoen.

De externe validiteit wordt geborgd door voldoende organisaties te onderzoeken en te zorgen dat deze organisaties representatief zijn voor de sector die zij vertegenwoordigen. Voor dit onderzoek zullen er zoveel mogelijk organisaties worden onderzocht, met als streven tussen de 100 en 150 organisaties.

Dit onderzoek is gebaseerd op publiek beschikbare informatie, zoals privacyverklaringen, jaarverslagen en organisatiewebsites. Alhoewel de GDPR aan organisaties verplicht om open en transparant om te gaan in hun gebruik en processen met betrekking tot persoonsgegevens, wil dat niet per definitie zeggen dat dit naar voren komt in de onderzochte privacy statements en jaarverslagen. Daardoor kan een verschil bestaan tussen de daadwerkelijke implementatie van de GDPR en de wijze waarop over privacy en GDPR gecommuniceerd wordt.

3.4.2. Betrouwbaarheid

Door gebruik te maken van expliciete criteria waarmee wordt bepaald of een organisatie aan de gestelde voorwaarden heeft voldaan, wordt de betrouwbaarheid van dit onderzoek geborgd. Daarbij wordt in Appendix 3 ook vermeld wat de factoren zijn die onderzocht worden en het protocol waarmee de score voor deze factoren bepaald wordt.

3.4.3. Ethische verantwoording

Dit onderzoek heeft als doel om een mogelijk verschil in grondigheid van GDPR-implementaties tussen de overheid, semioverheid en private sector aan te tonen. Daarmee spreken de resultaten niet voor individuele organisaties en hun implementaties. Het is van belang om de uitkomsten over

de gehele linie te zien, omdat de kracht van dit kwantitatieve onderzoek ligt in de indicatie van grondigheid van implementatie per sector. Daarnaast moeten de resultaten gezien worden als een momentopname, aangezien de grondigheid van GDPR-implementaties in verloop van tijd kan af- of toenemen.

4. Resultaten

4.1. Uitvoering onderzoek

Het verzamelen van data is zonder noemenswaardige bijzonderheden verlopen. Van de meeste organisaties was de privacy statement goed vindbaar en ook de jaarverslagen waren meestal gemakkelijk te vinden. Daarbij viel wel op dat voor de publieke sector, veelal voor gemeenten, een website werd gebruikt als jaarverslag. Dat maakte het verzamelen van gegevens zoals het totaalaantal woorden van een jaarverslag in deze gevallen onmogelijk. Dat heeft als gevolg gehad dat er geen punten toegekend konden worden voor het percentage woorden dat aan de GPDR/privacy is besteed (zie 3.2.3, factor 2.2).

Verder is gedurende het onderzoek is het protocol voor de beoordeling van de factoren aangepast op punten waarover onduidelijkheid kan ontstaan. Zoals de mate waarin rechten benoemd worden en hoe de grootte van de organisatie gemeten wordt. Ook zijn de grenzen voor het toekennen van punten bepaald voor de factoren met een numerieke uitkomst, zoals het aantal woorden besteed aan privacy en het aantal gevonden privacygerelateerde trefwoorden. Deze grenzen zijn te vinden in Appendix 3.

4.2. Resultaten

Voor dit onderzoek zijn er 152 organisaties onderzocht op de mate waarin zij de GDPR grondig hebben geïmplementeerd. Omdat de twee onafhankelijke variabelen de ‘Sector’ en ‘Organisatiegrootte’ zijn. Voor de factor ‘Sector’ is er onderscheid gemaakt tussen ‘Privaat’, ‘Semipubliek’ en ‘Publiek’. Voor de factor ‘Organisatiegrootte’ is er een onderscheid tussen ‘Klein’ en ‘Groot’. De verdeling van organisaties over deze factoren is te zien in Tabel 1.

Tabel 1 Kruisvergelijking sector en organisatiegrootte

		Organisatiegrootte		
		Klein	*Groot*	*Totaal*
Sector	*Privaat*	16	46	62
	Semipubliek	8	20	28
	Publiek	53	9	62
	Totaal	77	75	

In Tabel 1 valt op dat de verdeling van organisaties van sectoren ten opzichte van organisatiegrootte niet gelijkmatig verdeeld is. In de regressieanalyse zal hiermee rekening gehouden worden in verband met mogelijk multicollineariteit.

Wat betreft de factoren ten opzichte van de score is de verdeling zoals te zien in Tabel 2.

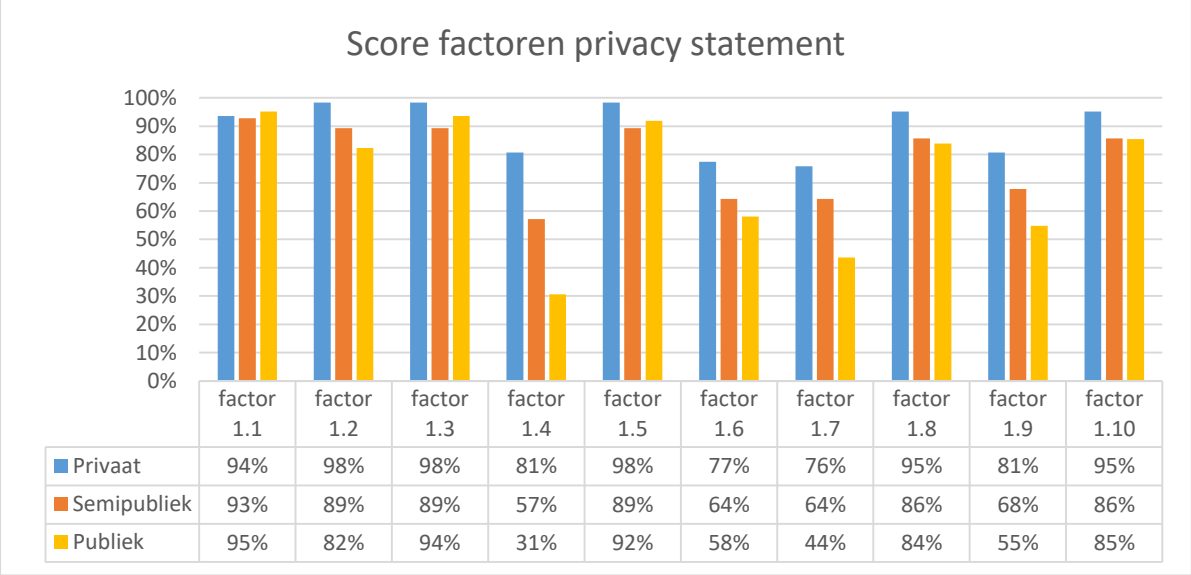
Tabel 2 Omschrijvende statistiek, sectoren en organisatiegrootte ten opzichte van score

	N	Gemiddelde	Mediaan	Standaard-afwijking	Range	Minimum	Maximum
Sector							
Privaat	62	10,45	10	2,82	15	0	15
Semipubliek	28	10,07	11	3,50	13	1	14
Publiek	62	8,53	9	2,87	13	2	15
Organisatiegrootte							
Klein	77	8,92	9	3,00	13	2	15
Groot	75	10,29	10	3,04	15	0	15
Totaal							
Totaal	152	9,60	10	3,09	15	0	15

Bij de omschrijvende statistiek van de score wordt er verder gekeken of deze waarde een normale verdeling heeft. Dat gebeurt aan de hand van de skewness (scheefheid) en kurtosis (bolling) van de verdeling. Beiden moeten, als zij gedeeld worden door de standaardafwijking, tussen -1,96 en 1,96 liggen om als normale verdeling gezien te worden.

Voor de verdeling van de resultaten van alle sectoren is er geen sprake van een normale verdeling, want skewness = -,597 en standaardafwijking = ,197 komt uit op -3,03 en dat valt buiten de marge. De bolling valt wel binnen de marge met kurtosis = ,27 en standaardafwijking = ,391, wat uitkomt op 0,69. Als enkel naar de sectoren publiek en privaat wordt gekeken en semipubliek wordt uitgesloten, is er wel sprake van een normale verdeling, met skewness = -,413 en standaardafwijking = ,217 is de uitkomst -1,903. En voor kurtosis = ,232 met standaardafwijking = ,431 een uitkomst van 0,538.

In Grafiek 1 is de scoreverdeling te zien van de factoren die betrekking hebben op de privacyverklaring. Het percentage van organisaties dat een punt heeft behaald wordt per factor getoond.



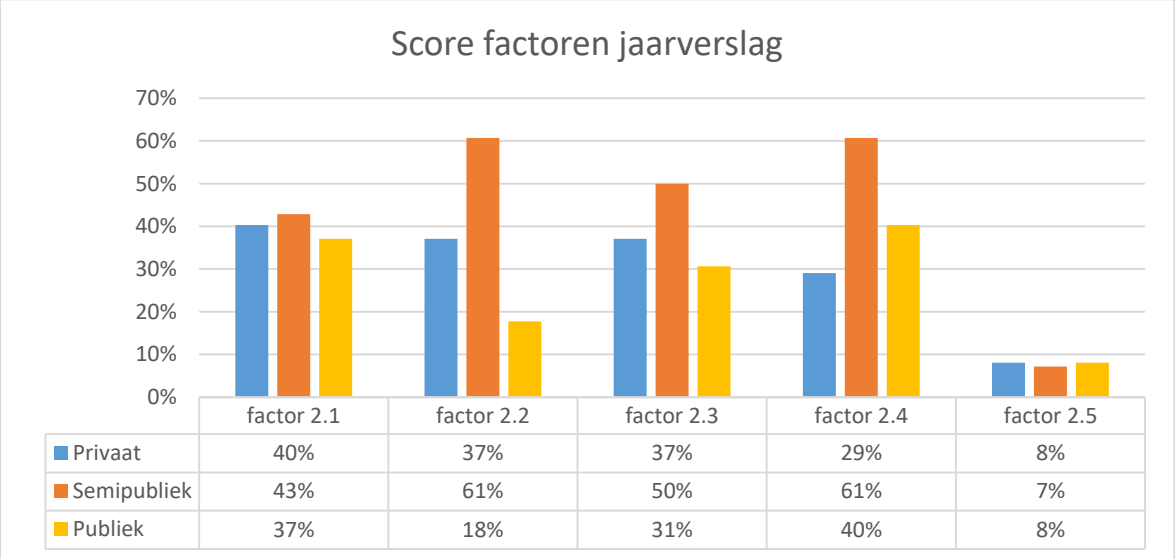
	factor 1.1	factor 1.2	factor 1.3	factor 1.4	factor 1.5	factor 1.6	factor 1.7	factor 1.8	factor 1.9	factor 1.10
Privaat	94%	98%	98%	81%	98%	77%	76%	95%	81%	95%
Semipubliek	93%	89%	89%	57%	89%	64%	64%	86%	68%	86%
Publiek	95%	82%	94%	31%	92%	58%	44%	84%	55%	85%

Grafiek 1 Scoreverdeling factoren privacy statement

Te zien is dat de semipublieke sector in veel gevallen tussen het percentage van de private en de publieke sector scoort. Van de publiek en private sector is het onderlinge verschil het grootste voor

factor 1.4 (Recht op dataportabiliteit), waar de sector 'Publiek' duidelijk slechter scoort dan de sector 'Privaat'. Datzelfde geldt in mindere mate ook voor de factoren 1.7 (Recht op beperking van gegevensverwerking), 1.6 (Recht op bezwaar) en 1.9 (Mogelijkheid klacht Autoriteit Persoonsgegevens).

In Grafiek 2 is de scoreverdeling van de factoren die betrekking hebben op het jaarverslag te zien. Hierin valt op dat er over de gehele linie minder goed gescoord wordt dan voor de factoren in het privacy statement. Tussen 'Publiek' en 'Privaat' is het grootste onderlinge verschil zichtbaar in factor 2.2 (Percentage van jaarverslag besteed aan privacy), waarbij 'Publiek' lager scoort. Wat verder opvalt is dat de sector 'Semipubliek' in vier van de vijf gevallen beter scoort dan de publieke en private sector.



	factor 2.1	factor 2.2	factor 2.3	factor 2.4	factor 2.5
Privaat	40%	37%	37%	29%	8%
Semipubliek	43%	61%	50%	61%	7%
Publiek	37%	18%	31%	40%	8%

Grafiek 2 Scoreverdeling factoren jaarverslag

One way ANOVA

De one way ANOVA (F-test) test of er statistisch significante verschillen zitten tussen de gemiddelden van meerdere (onafhankelijke) groepen. Er is aangetoond dat er een significant verband zit tussen de sector en de score ($f(2, 86)= 6{,}896^{***}$, p= ,001). Daarom wordt de sector verder geanalyseerd in independent sample t-tests. De organisatiegrootte wordt niet behandeld in de One way ANOVA aangezien deze met twee klassen ('Klein' en 'Groot') al in de t-test geanalyseerd wordt.

Independent sample t-test

In een independent sample t-test worden de uitkomsten van de One way ANOVA verder geanalyseerd, door te kijken welke waarden binnen de categorieën significant van elkaar verschillen. Daarvoor worden voor elke independent sample t-test twee subgroepen met elkaar vergeleken. Voor dit onderzoek is een aantal van deze testen uitgevoerd, waarvan de volgende testen de meest relevante zijn.

Eén van de independent sample t-tests was tussen de groepen 'Privaat' en 'Publiek', om te testen of de verschillen in score te wijten kunnen zijn aan willekeur. Waarvan $t(124)= 3.76^{***}$, p= ,000, met een associatie met de private sector met een hogere score (Privaat= 10,45 en Overheid= 8,53).

De uitkomst van de independent sample t-test tussen 'Semipubliek' en 'Publiek' is als volgt. $T(90)= 2{,}2^{**}$, p= ,03. Met daarbij een associatie voor een hogere score voor de semioverheid (Semioverheid= 10,07 en Overheid= 8,53). De t-test levert geen significant resultaat op bij een vergelijking tussen privaat en semioverheid.

Daarnaast is er een independent sample t-test uitgevoerd voor variabele 'Organisatiegrootte' tussen de waarden 'Klein' (1) en 'Groot' (2). Daaruit komt t(152)= 2,8***, p= ,006, met een significante associatie van de groep met grotere organisaties met een hogere score (Groot (2)= 10,29 en Klein (1)= 8,92).

Bivariate correlaties

Uit de bivariate correlaties blijkt of en in welke mate variabelen een onderlinge samenhang vertonen. Daarvoor zijn de variabelen 'Sector', 'Organisatiegrootte' en 'Score' geanalyseerd.

Allereerst blijkt daaruit dat de 'Sector' en 'Organisatiegrootte' in deze dataset aan elkaar correleren met een Pearson correlatie van -,553*** (p= ,000). Dat wil zeggen dat er een aanzienlijke correlatie zit tussen de sector en de organisatiegrootte. Bij voorkeur was deze score lager geweest, zodat deze variabelen meer los van elkaar geanalyseerd kunnen worden. Hiermee wordt rekening gehouden in de regressie bij het bepalen van het modererend effect van de organisatiegrootte.

De correlatie van 'Sector' met 'Score' is met een Pearson correlatie van -,282***, p= ,000 ook duidelijk aanwezig. Evenals de correlatie van 'Organisatiegrootte' en 'Score' met een Pearson correlatie van -,269***, p= ,001.

Regressie

In de regressietest wordt geanalyseerd in welke mate variabelen elkaar verklaren of voorspellen. Omdat er in dit onderzoek meerdere factoren zijn gemeten, worden deze ook meegenomen in de analyse om multicollineariteit te bepalen. Daarmee wordt onderzocht of de voorspellende variabelen onderling mogelijk (sterk) gecorreleerd zijn.

In de analyse is allereerst gekeken hoe de regressie over de sector in verhouding tot de score kan worden uitgevoerd, daarbij is gekozen om 'Semipubliek' in de regressie buiten beschouwing te laten, zodat de Adjusted R Square van ,72 stijgt tot ,96. Zie Tabel 3 voor de resultaten van deze analyse.

Tabel 3 Regressieanalyse sector t.o.v. score

Model samenvatting

R Square	,104
Adjusted R Square	,096

ANOVA

F	14,12***
p	,000

Coefficients

	ß	**t**	**p**
Constant (Publiek)	8,53***	23,62	0,000
Privaat	1,92***	3,76	0,000

Voor de regressieanalyse voor de variabele 'Organisatiegrootte' ten opzichte van de score, zijn resultaten van de semioverheid eveneens buiten beschouwing gelaten. Daaruit komen de resultaten zoals te zien in Tabel 4.

Tabel 4 Regressieanalyse organisatiegrootte t.o.v. score

Model samenvatting

R Square	,077
Adjusted R Square	,069

ANOVA

F	10,18***
p	,002

Coëfficiënten

	ß	**t**	**p**
Constant (Klein)	8,75 ***	25,19	0,000
Groot	1,67***	3,19	0,002

Wanneer zowel de organisatiegrootte ('Klein' en 'Groot') als de sector 'Publiek' en 'Privaat' wordt meegenomen in een regressieanalyse, leidt dat tot de analyse in Tabel 5.

Tabel 5 Regressieanalyse sector en organisatiegrootte t.o.v. score

Model samenvatting

R Square	,115
Adjusted R Square	,100
Durbin-Watson	1,88

ANOVA

F	7,85***
p	,001

Coëfficiënten

	ß	**t**	**p**	**VIF**
Constant (Publiek-Klein)	8,42 ***	22,61	0,000	
Privaat	1,45**	2,27	0,025	1,564
Groot	,79	1,23	0,221	1,564

In het model is de VIF 1,564, waarmee het geen indicatie geeft van multicollineariteit. Ook wijst de Durbin-Watson waarde van 1,879 niet op een correlatie tussen de errors (residual) in het model.

Modererend effect

Om de mate van het modererend effect te bepalen wordt de PROCESS-macro (Processmacro.org, sd) in SPSS gebruikt. Hiervoor worden enkel de sectoren 'Publiek' en 'Privaat' gebruikt omdat in de eerdere regressies bleek dat het meenemen van 'Semipubliek' ten koste gaat van de kwaliteit van het model. De resultaten uit Tabel 6 komen uit de analyse met de PROCESS-macro.

Tabel 6 Modererend effect (PROCESS-macro) organisatiegrootte

Model samenvatting (afhankelijke variabele: Score)

Model	1
Y	Score
X	Sector-Privaat
W	Grootte-Groot
Sample size	124

R	**R-square**	**MSE**	**F**	**P**
0,34	0,12	8,10	5,29	0,002

Model

	Coëfficiënt	**Standaard-afwijking**	**t**	**P**
Constant (Publiek, Klein)	8,36***	,39	21,38	,000
Privaat	1,70**	,81	2,10	,038
Groot	1,20	1,03	1,17	,246
Int_1 *(Privaat * Groot)*	-,67	1,32	-,51	,611

Interacties

	R-square-change	**F**	**P**
X*W	,002	,26	,611

De verklaarde variantie van het model is significant, R^2= ,117***, F(3, 120)= 5,285, p= ,002. Dit is te zien bij *Model samenvatting*. Het onderscheid tussen overheid en de private sector is een significante voorspeller in het model, b1= 1,704**, t= ,812, p= ,038, zoals ook was vastgesteld in de independent sample t-tests. De organisatiegrootte is geen significante voorspeller voor de score, b2= 1,197, t= 1,026, p= ,246. Dit is te zien onder het kopje *Model*.

Verder is te zien dat de interactie tussen de sector en de organisatiegrootte met p= 0,611 niet significant is en geen toegevoegde waarde heeft voor het model. Dit is te zien onder het kopje *Interacties*.

5. Conclusie, discussie en aanbevelingen

5.1. Conclusie

Voor dit onderzoek was de hoofdvraag in hoeverre de sector waartoe een organisatie behoort (publiek/semipubliek/privaat) voorspellend is voor de mate van grondigheid van hun GDPR-implementatie. Daarbij is de grootte van de organisatie meegenomen als modererende variabele. Uit de resultaten blijkt dat organisaties uit de publieke sector gemiddeld 8,53 scoren op grondigheid, waar dat voor de semipublieke sector 10,07 en voor de private sector 10,45 is. De standaardafwijking is voor zowel de publieke als de private sector rond de 2,80. Dat het resultaat uit de t-test tussen de semipublieke en de private sector niet significant was, is mogelijk een teken dat het gemiddelde van de semipublieke sector minder betrouwbaar is. Een waarschijnlijke oorzaak daarvan is de kleinere hoeveelheid organisaties in de semipublieke sector met een grotere standaardafwijking (3,49).

Ook kwam uit de resultaten dat de kleinere organisaties uit dit onderzoek gemiddeld een 8,92 scoorden, waar de grotere organisaties uitkwamen op 10,29. Beiden met een standaardafwijking rond de 3,0. Over alle organisaties gezien was het gemiddelde een 9,60 met een standaardafwijking van net boven de 3,0.

Hoewel uit de bivariate correlaties bleek dat er een aanzienlijke overlap was tussen zowel de publieke sector en kleine organisaties, als tussen de private sector en grote organisaties, kwamen er uit de regressieanalyse geen scores die erop duiden dat er sprake was van multicollineariteit. De modererende factor kwam in dit onderzoek tot een waarde van -,67, maar bleek verre van significant met een p van 0,61.

Wat betreft de hypotheses kan gesteld worden dat H1a is verworpen, aangezien organisaties binnen de publieke sector niet hoger, maar lager scoren op grondigheid van GDPR-implementatie. Hypothese H1b kan worden aanvaard, aangezien de semipublieke sector tussen de publieke en private sector zit in score voor grondigheid. Voor hypothese H2 is geen significant resultaat, waardoor deze hypothese niet wordt aanvaard of verworpen.

Wat betreft de onderzoeksvraag van dit onderzoek kan er geconcludeerd worden dat de sector waartoe een organisatie behoort van invloed is op de score voor de grondigheid van de GDPR-implementatie. Waarbij de semipublieke sector ruim 1,5 punt hoger scoort dan de publieke sector, en de private sector nog hoger scoort met gemiddeld ruim 1,9 punt hoger dan de publieke sector.

5.2. Discussie – reflectie

Vanuit de literatuur kwam een aantal verwachtingen over de onderzoeksresultaten. Op basis van institutionele theorie werd verwacht dat resultaten voor organisaties binnen de onderzochte sectoren meer op elkaar zouden lijken dan de resultaten van organisaties tussen verschillende sectoren (DiMaggio & Powell, 1983). Verklaringen die de literatuur hiervoor geeft zijn onder meer de intensievere focus en controle op de publieke sector voor het voldoen aan de GDPR (coercive), het vervullen van een voorbeeldfunctie in het voldoen aan wet- en regelgeving voor de overheid (normative) en het volgen van (best) practices die binnen de sectoren met soortgelijke organisaties worden gedeeld (mimetic) (Mebius, 2018). Hoe de resultaten zouden uitvallen, behalve dat deze per sector zeer waarschijnlijk zouden verschillen, was uit de literatuur niet met zekerheid te voorspellen.

Eerder onderzoek wees zowel in de richting van een publieke sector die hoger zou scoren, als in de richting dat de private sector een hogere score zou behalen (Chua, Herbland, Wong, & Chang, 2017) (Luoma-aho, 2008) (Baarspul & Wilderom, 2012, Volume 13, Uitgave 7). Daarnaast kan het zijn dat de publieke sector de eerste jaren van de GDPR strenger gecontroleerd zou worden op compliance door de Autoriteit Persoonsgegevens niet alleen gebaseerd was op het gebruik van persoonsgegevens en hun voorbeeldfunctie (Mebius, 2018). Maar dat een andere overweging hierin was dat de publieke sector, bijvoorbeeld op basis van eerdere ervaringen, een hoger risico heeft op het niet voldoen aan (privacy)wetgeving.

Daarnaast zou het model voor institutionele theorie ook gevuld kunnen worden met krachten van sectoren die de kant op zouden wijzen van een hogere compliance door de private sector. Denk daarbij aan het voorkomen van boetes die ten koste kunnen gaan van de winst (coercive), het voldoen aan het imago waarbij persoonsgegevens veilig zijn bij private organisaties (normative) en het wendbaarder en sneller kunnen reageren op veranderende omstandigheden (mimetic). Wat dat betreft is institutionele theorie beter geschikt als een verklarende dan een voorspellende theorie.

Bij het verzamelen van de onderzoeksdata viel een aantal zaken op. Zo leek het, ondanks dat dit geen onderzoeksvariabele was, dat organisaties die minder met persoonsgegevens te maken hebben over het algemeen laag scoorden. Dat is eenvoudig te verklaren gezien de aard van de GDPR, maar in dit onderzoek zou dat wellicht een deel van de variatie binnen de onderzoeksvariabelen kunnen verklaren. Wat bij dergelijke organisaties veelal voorkwam, was dat de privacyverklaring niet als organisatie was opgesteld, maar specifiek voor de website gold.

Daarnaast viel het verschil in de mate waarin rechten werden genoemd in de privacyverklaringen op. Zo was er bij sommige gevallen te zien dat een uitgebreide omschrijving van privacyrechten eenzelfde score kreeg als organisaties die in hun privacyverklaring niet veel verder kwamen dan het benoemen van de rechten. Een veel geziene tekst van de privacyverklaringen voor het omschrijven van rechten kwam neer op *'Gegevens inzien, aanpassen of verwijderen'*, of een soortgelijke variant. Dit heeft in veel gevallen structureel puntenverlies opgeleverd, aangezien de andere rechten (dataportabiliteit, bezwaar, beperking op gegevensverwerking) dan vaak niet genoemd werden. Ook was te zien dat bepaalde organisaties simpelweg meer moeite steken in de communicatie naar de buitenwereld, wat ertoe kan leiden dat ondanks een minder grondige GDPR-implementatie op de achtergrond, de intensievere communicatie over de GDPR extra punten opleverde.

De inzichten die dit onderzoek heeft opgeleverd zijn door de opzet niet erg fijnmazig, maar geven over de onderzochte sectoren als geheel wel een overtuigend beeld van een verschil in grondigheid met betrekking tot de GDPR-implementaties. Waar uit de literatuur die is meegenomen in deze studie geen eenduidig beeld geschetst kon worden over de richting waarin de resultaten van dit onderzoek zouden vallen, laten de resultaten van dit onderzoek duidelijk zien dat overheidsorganisaties over de gehele linie minder goed scoren op de gemeten factoren.

Wat daarbij als kanttekening geplaatst kan worden, is dat de privacyrechten in de GDPR geen absolute rechten zijn en dat deze kunnen worden afgewogen tegenover bijvoorbeeld een wettelijke verplichting van een organisatie om persoonsgegevens te verwerken, ongeacht een verzoek tot 'beperking van gegevensverwerking' or 'vergetelheid'. In dit onderzoek is daarin tussen organisaties geen onderscheid gemaakt, maar dat kan gezien het grote aantal gemeenten wel zijn dat deze nuance een rol heeft gespeeld in de vorming van hun privacyverklaringen.

Na het uitvoeren van dit onderzoek zijn er ook dingen die in een vervolg anders aangepakt zouden worden. Een goed voorbeeld daarvan is de selectie van organisaties, waarbij meer rekening gehouden had kunnen worden met de overlap van sector en organisatiegrootte. Omdat gemeenten veelal kleine organisaties zijn volgens dit onderzoek, en beursgenoteerde bedrijven meestal grote organisaties zijn, had de selectie van organisaties beter in balans kunnen zijn. Ondanks dat uit de statistische tests geen multicollineariteit is vastgesteld, hadden de organisaties meer bewust verdeeld kunnen worden over de selectievariabelen. Daarnaast zouden er om meer diepte te geven aan de analyse meer selectievariabelen uitgekozen kunnen worden. En ondanks dat dit momenteel nog niet mogelijk was, zou in een vervolgonderzoek nadrukkelijker de link gelegd worden tussen de gemeten factoren en de daadwerkelijke grondigheid van implementatie. Dat de GDPR ondertussen bijna twee jaar van kracht is, maakt dat er steeds meer onderzoek beschikbaar komt om een onderzoek als dit in te nabije toekomst beter vorm te geven en te interpreteren.

5.3. Aanbevelingen voor de praktijk

Voor de praktijk biedt dit onderzoek een aantal aanbevelingen:

- Gebruik best practices/templates voor privacy statements die een volledig beeld geven van privacyrechten;
  In veel gevallen lijkt de reden van tekortkomingen dat organisaties niet goed weten wat ze over de privacyrechten moeten uitdragen naar lezers van hun privacy statements. Hierdoor worden in sommige gevallen rechten niet of nauwelijks benoemd, en komt een deel van de organisaties niet verder dan 'het recht om gegevens in te zien, aan te passen of te verwijderen'. Door een voorbeeld te bieden waarin alle rechten staan, geeft dat organisaties ook de duidelijkheid dat van hen verwacht wordt dat zij hieraan voldoen. Wat in veel gevallen leidt tot de benodigde wijzingen in de daadwerkelijke implementatie voor de GDPR.

- Benoem ook de privacyrechten die niet of verminderd van toepassing zijn in privacyverklaringen;
  Reden van structureel puntenverlies was mogelijk dat sommige organisaties rechten niet benoemden, met als reden dat de rechten niet of minder van toepassing zijn in de specifieke situatie van de organisatie. Denk daarbij aan gemeenten, die bijvoorbeeld niet altijd kunnen ingaan op het recht op beperking van gegevensverwerking of op het recht van dataportabiliteit. Door dit niet te benoemen is voor lezers niet helder of dit recht van toepassing is en zo niet, waarom niet. In het kader van transparantie en volledigheid kan er gekozen worden om rechten wel te vermelden en hier dan als voetnoot bij te zetten dat het gebruik van de privacyrechten aan voorwaarden of beperkingen gebonden kan zijn.
- Geef meer voorbeelden over de wijze waarop de GDPR bij organisaties geïmplementeerd kan worden;
  Dat er ruimte is voor interpretatie wat betreft de implementatie van de GDPR, kan leiden tot onduidelijkheid van wat er verwacht wordt en welke delen verplicht zijn. Door het voortouw te nemen in het vormen van een 'generieke' vorm van GDPR-implementatie, kan de norm gezet worden dat er daarmee voldaan wordt aan de GDPR. Uit de dataverzameling van dit onderzoek blijkt dat zeker organisaties die minder met persoonsgegevens werken, hierin steun kunnen gebruiken.
- Besteed aandacht aan privacy in jaarverslagen;
  In de jaarverslagen kwam naar voren dat voor een deel van de organisaties, privacy geen onderwerp was waarover zij actief communiceren. Door privacy bijvoorbeeld als hoofdstuk of onderwerp mee te nemen in jaarverslagen, wordt ook naar personen buiten de organisatie gecommuniceerd dat er bewust over privacy wordt nagedacht en compliant met persoonsgegevens wordt omgesprongen.

5.4. Aanbevelingen voor verder onderzoek

Voor toekomstig onderzoek zijn is de voornaamste aanbeveling om de koppeling te leggen tussen kwalitatieve kenmerken van GDPR-implementaties en de factoren die vanuit publieke bronnen te meten zijn. Wanneer er een link wordt gelegd die valideert dat de gemeten factoren samenhangen met een grondige implementatie in de praktijk, biedt het dit (soort) onderzoek meer validiteit en biedt het de mogelijkheid om in toekomstig onderzoek wellicht hardere conclusies uit soortgelijke data te kunnen trekken.

Verder is meer onderzoek naar de GDPR en implementatiestrategieën van organisaties nodig, wat op het moment van dit onderzoek nauwelijks beschikbaar was gezien de recente ingang van de wetgeving. Op het gebied van privacy zou dat ook een toevoeging zijn van meer Europees onderzoek aangezien de meest vooraanstaande papers over privacy uit de Verenigde Staten komen, de GDPR vanzelfsprekend een minder onderzocht onderwerp is.

In toekomstig onderzoek zou het ook van waarde zijn als er specifiekere variabelen worden gekozen. Dat zou in het verlengde van dit onderzoek in plaats van 'publieke sector' bijvoorbeeld een onderscheid tussen de lokale en de centrale overheid kunnen zijn. Of bij de 'semipublieke sector' een onderscheid tussen 'zorg', 'onderwijs', 'nutsbedrijven', et cetera. Verder komen er meer factoren beschikbaar die het mogelijk maken die gebruikt kunnen worden als indicatief voor de grondigheid van GDPR-implementatie, zoals opgelegde boetes en behaalde AVG-certificering. En ten slotte zouden eventueel factoren mee kunnen worden genomen die in dit onderzoek buiten beschouwing zijn gelaten, zoals de hoeveelheid persoonsgegevens die organisaties verwerken.

6. Referenties

Almanak Overheid. (sd). Opgehaald van overheid.nl: https://almanak.overheid.nl/

Autoriteit Persoonsgegevens, AP doet handreikingen om registratie datalekken te verbeteren. (2018). Opgehaald van Autoriteitpersoonsgegevens.nl: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handreiking_verbeteren_registratie_datalekken.pdf

Autoriteit Persoonsgegevens, Privacyrechten. (sd). Opgehaald van Autoriteit Persoonsgegevens, Privacyrechten: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten

Baarspul, H. C., & Wilderom, C. P. (2012, Volume 13, Uitgave 7). Do employees behave differently in public vs private organizations? *Public Management Review*, 967-1002.

Birnhack, M., & Elkin-Koren, N. (2010). Does Law Matter Online-Empirical Evidence on Privacy Law Compliance. *Mich. Telecomm. & Tech. L. Rev., 17*, 337.

Centraal Bureau voor de Statistiek. (2018). *Wat rekent het CBS tot de sector overheid?*

Christmann, P., & Taylor, G. (2006). Firm Self-Regulation through International Certifiable Standards: Determinants of Symbolic versus Substantive Implementation. *Journal of International Business Studies, 37*(6), 863-878.

Chua, H., Herbland, A., Wong, S., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics, 34*(4), 157-170.

de Vries, J., & Sys, M. (2019, Mei 24). Publieke sector wordt belemmerd door privacywet - en dat leidt tot gevaarlijke situaties. *De Volkskrant*. Opgehaald van https://www.volkskrant.nl/nieuws-achtergrond/publieke-sector-wordt-belemmerd-door-privacywet-en-dat-leidt-tot-gevaarlijke-situaties~b814ab27/

DiMaggio, P. J., & Powell, W. W. (1983, April). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review, 48*(2), 147-160. doi:10.2307/2095101

Garber, J. (2018). GDPR - compliance nightmare or business opportunity? *Computer Fraud & Security, 2018*(6), 14-15. doi:10.1016/S1361-3723(18)30055-1

Hofmans, T. (2019, April 18). *Belastingdienst voldoet na jaar nog steeds niet aan AVG - update*. Opgehaald van Tweakers.net: https://tweakers.net/nieuws/151770/belastingdienst-voldoet-na-jaar-nog-steeds-niet-aan-avg.html

London Chamber of Commerce and Industry. (2018, januari 22). One in four London businesses unaware of new data protection regulation. *London Chamber of Commerce and Industry*. Opgehaald van https://www.londonchamber.co.uk/news/press-releases/one-in-four-london-businesses-unaware-of-new-data/

Luoma-aho, V. (2008). Sector reputation and public organisations. *International Journal of Public Sector Management, 21*(5), 446-467. doi:10.1108/09513550810885778

Mebius, D. (2018, mei 25). Privacywaakhond heeft te weinig handhavers voor kleine bedrijven; vooral controle overheid en zorg. *De Volkskrant*. Opgehaald van

https://www.volkskrant.nl/nieuws-achtergrond/privacywaakhond-heeft-te-weinig-handhavers-voor-kleine-bedrijven-vooral-controle-overheid-en-zorg~b81129ed/

Pavlou, P. A. (2011). State Of The Information Privacy Literature: Where Are We Now And Where Should We Go? *MIS Quarterly, 35*(4), 977-988. doi:10.2307/41409969

Processmacro.org. (sd). Opgehaald van Processmacro.org: http://processmacro.org/index.html

Rossi, A. (2018, oktober). How the Snowden Revelations Saved the EU General Data Protection Regulation. *The International Spectator, 53*(4), 95 - 111. doi:10.1080/03932729.2018.1532705

Saunders, M., Lewis, P., & Adrian, T. (2016). *Research Methods for Business Students* (Seventh Edition ed.). Pearson.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 5-8. doi:10.1016/S1353-4858(16)30056-3

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 134-153. Opgehaald van http://search.ebscohost.com/login.aspx?direct=true&db=eoah&AN=42069046&site=ehost-live

7. Appendices

7.1. Appendix 1: Onderzoeksaanpak

7.1.1. Bronnen

De bronnen van die geraadpleegd worden zijn in vier groepen onder te verdelen:

1) Aangedragen bronnen vanuit de afstudeeropdracht. Dit betreft basisliteratuur over soortgelijke onderzoeken;
   Dit zijn de bronnen direct door de Open Universiteit aangedragen, in zowel de basisopdracht als in latere studiebijeenkomsten.

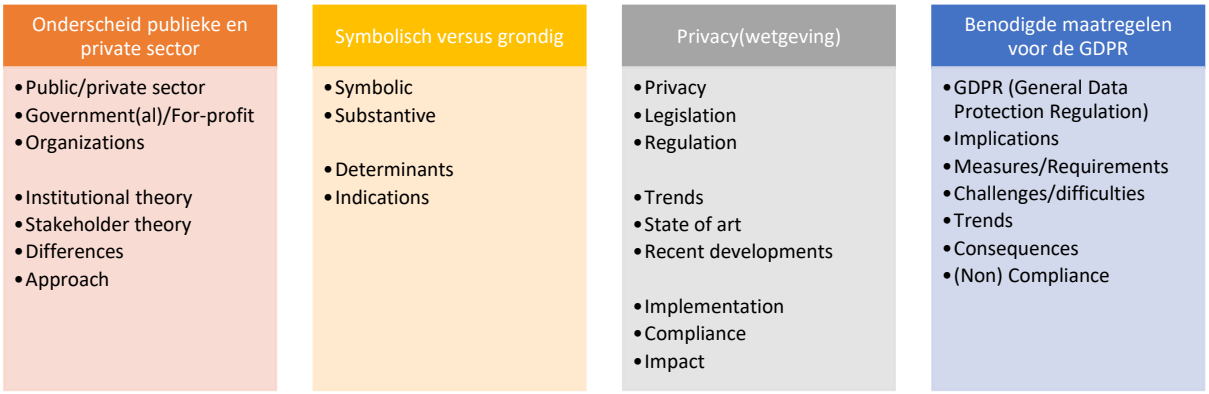
2) Bronnen gevonden door zoekopdrachten die zijn gedaan op databases van wetenschappelijke artikelen;
   Hierbij wordt gebruik gemaakt van drie wetenschappelijke databases:
   - *Google Scholar (https://scholar.google.nl);*
   - *De onlinebibliotheek van de Open Universiteit (https://bibliotheek.ou.nl);*
   - *EBSCO Host (https://search.ebscohost.com/).*

3) Bronnen die gevonden zijn door vanuit wetenschappelijke artikelen gebruik te maken van *forward* en *backward snowballing;*
   Voor deze methodiek wordt gebruik gemaakt van de referenties van artikelen. Hier wordt met forward snowballing bedoeld dat er gezocht wordt naar artikelen waarin een bepaald wetenschappelijk artikel geciteerd wordt. Met backward snowballing wordt bedoeld dat gebruikte bronnen van een wetenschappelijk artikel zijn geraadpleegd, zodat onderliggende theorieën van geraadpleegde literatuur kunnen worden getraceerd.

4) Bronnen in de vorm van nieuwsartikelen. Deze worden gevonden door op (geaggregeerde) nieuwssites te zoeken op zoektermen.
   Ten slotte worden nieuwsartikelen als bron gezocht. In nieuwsartikelen kunnen recente trends worden omschreven waarvoor nog geen wetenschappelijke onderbouwing beschikbaar is. In het geval van de GDPR is dit een nuttige bron, aangezien over de GDPR nog geen tot weinig concrete wetenschappelijke artikelen zijn over hoe de implementatie hiervan voor organisaties is verlopen. Nieuwsartikelen worden in dit onderzoek gevonden door te zoeken op Google Nieuws (https://news.google.nl), waar met één zoekopdracht resultaten uit meerdere nieuwsbronnen getoond worden.

7.1.2. Zoektermen

De zoektermen die worden gebruikt zijn gebaseerd op de hoofdonderwerpen dat in het doel van het theoretisch kader (2.1.1) staan omschreven. Door per onderwerp zoektermen te clusteren, ontstaat het volgende overzicht (Figuur 1). Hierin is te zien welke zoektermen per onderwerp zijn gebruikt. Deze zoektermen staan in het Engels vermeld, omdat de meeste artikelen Engelstalig zijn, maar er is ook op de Nederlandse vertaling van die zoektermen gezocht. Er is gezocht op zowel losse termen als op combinaties hiervan.



Figuur 1 Overzicht zoektermen per onderwerp

Deze zoektermen zijn bij de verschillende bronnen gebruikt. Waaruit vervolgens een selectie is gemaakt van relevante artikelen.

7.1.3. Relevantie van gevonden literatuur

De relevantie van de gevonden artikelen wordt bepaald op basis van een aantal voorwaarden. Deze voorwaarden zijn richtinggevend, maar niet bepalend. Wanneer er (nog) niet veel onderzoek is gedaan in een bepaalde richting, betekent dat dat de voorwaarden soms soepeler gehanteerd worden. Denk daarbij aan artikelen over de GDPR, die nuttig kunnen zijn, maar waarschijnlijk nog nauwelijks zijn geciteerd gezien de recente aard van de verordening.

Bij het zoeken naar bronnen geeft Tabel 1 aan op welke wijze relevantie wordt bepaald in de zoekresultaten.

Tabel 1 Relevantie van gevonden literatuur

Kenmerk	Voorkeur
Onderwerp	Titel en inhoud komen zoveel mogelijk overeen met het onderwerp waarop werd gezocht
Bruikbaarheid	De gevonden literatuur moet bijdragen aan de onderbouwing van dit onderzoek
Kwaliteit van journal	Kwaliteitsjournals krijgen de voorkeur
Aantal maal geciteerd	De voorkeur gaat uit naar artikelen die vaker zijn geciteerd
Moment van publicatie	Er wordt zoveel mogelijk recente literatuur gebruikt
Taal	Engelstalig of Nederlandstalig
Plaats in zoekresultaten	In het geval van veel zoekresultaten, zal er niet verder worden gekeken dan hooguit de tweede resultatenpagina.
Aard van de bron	Er wordt in de vereisten een onderscheid gemaakt tussen theorieën, onderzoeken en nieuws- en magazineartikelen. Bijvoorbeeld in *aantal keer geciteerd* en het *moment van publicatie*.

7.2. Appendix 2: Selectie van organisaties

7.2.1. Bepaling sectoren

In de dataset worden organisaties onderverdeeld onder de categorieën ‘Privaat’, ‘Semipubliek’ en ‘Publiek’. In de dataset zal dat worden omgezet naar de nominale waarden 1 (Privaat), 2 (Semipubliek) en 3 (Publiek).

Voor organisaties uit de private sector wordt enkel geselecteerd op beursgenoteerde organisaties. Deze zijn online goed vindbaar, hebben veelal jaarverslagen beschikbaar en van deze organisaties mag gezien de omvang ook verwacht worden dat zij zich actief bezighouden met maatregelen voor de GDPR.

Voor organisaties uit de overheidssector wordt een selectie gemaakt uit lokale overheid (gemeenten/provincies) en centrale overheid (ministeries, rijksoverheidsorganisaties). (Almanak Overheid, 2019)

Voor organisaties van de semioverheid wordt gekeken naar zelfstandige bestuursorganen, zorginstellingen, onderwijsinstellingen, netbeheerders en waterbedrijven. (Almanak Overheid, 2019)

7.2.2. Verhouding sectoren

Het voornaamste onderscheid in het onderzoek zit tussen organisaties uit de publieke en private sector. De semipublieke sector wordt gezien als een tussenstap tussen de publieke en private sector, en speelt een kleinere rol in dit onderzoek.

Er wordt naar een verdeling gestreefd waarbij de publieke en de private sector beiden 40 procent van de onderzochte organisaties vormen, en de resterende 20 procent van de organisaties bestaat uit semioverheid. Tijdens de uitvoering van het onderzoek wordt deze verhouding bewaakt.

7.2.3. Organisatiegrootte

Het aantal medewerkers wordt vastgelegd om de grootte van de organisatie te meten. Dit wordt gedaan door op de website van de organisatie naar het aantal medewerkers te zoeken, in de jaarverslagen naar het aantal medewerkers van de organisatie te zoeken, op LinkedIn het aantal medewerkers van de organisatie op te zoeken of via een zoekmachine informatie te vinden over het aantal medewerkers van de organisatie.

Bij veel organisaties wordt het aantal werknemers expliciet vermeld, maar in sommige gevallen wordt dit niet in aantal personen maar in aantal fte’s (fulltime-equivalent) vermeld. Ook al staan werknemers en fte’s niet direct gelijk aan elkaar, zijn deze wel als één waarde overgenomen voor de grootte van de organisatie. De verhouding van het aantal fte’s ten opzichte van het aantal werknemers is per organisatie verschillend en kan dus niet eenduidig en correct overgezet worden naar aantal medewerkers.

Voor de analyse worden de organisaties ingedeeld in twee groepen. De verdeling van organisaties is als volgt.

Tabel 2 Verdeling organisatiegrootte

	Aantal organisaties	Aantal medewerkers
Klein	77	<= 1.700
Groot	75	> 1.700
Totaal	152	

7.3. Appendix 3: Dataverzameling scoreprotocol

7.3.1. Bronnen

Voor het verzamelen van data voor dit onderzoek, wordt gebruik gemaakt van openbare bronnen. De bronnen die worden geraadpleegd voor het scoren van de hieronder genoemde factoren zijn:

- Websites
- Privacy statements
- Jaarverslagen

7.3.2. Onderzochte factoren

Tabel 3 Factoren privacy statements

Privacy statement		**Score**
Factor 1.1	Aanwezigheid privacy statement *Door op de website van de organisatie te zoeken naar privacy, een privacy statement of een privacyverklaring wordt het privacy statement van een organisatie gevonden. Om een punt te verdienen moet er een (toegankelijk/begrijpelijk) privacy statement of privacyverklaring aanwezig zijn. Als er een webpagina over privacy is die dezelfde informatie biedt in een soortgelijke vorm als een privacy statement, telt dit ook als punt.* *Een verwijzing naar een privacybeleid, of een privacy statement in juridische taal, verdient geen punt.*	0-1 punt
Factor 1.2	Recht op informatie *Als in het privacy statement informatie wordt gegeven over (1) welke gegevens worden verzameld en (2) voor welke doeleinden deze gegevens verzameld worden, wordt er een punt toegekend. Dit gebeurt ook als in het privacy statement gewezen wordt op het recht van informatie.*	0-1 punt
Factor 1.3	Recht op inzage *Als in het privacy statement het recht op inzage wordt genoemd, wordt een punt toegekend.*	0-1 punt
Factor 1.4	Recht op dataportabiliteit *Als in het privacy statement het recht op dataportabiliteit (of gegevensoverdracht) wordt genoemd, wordt een punt toegekend.*	0-1 punt
Factor 1.5	Recht op rectificatie *Als in het privacy statement het recht op rectificatie, correctie of aanpassing wordt genoemd, wordt een punt toegekend.*	0-1 punt
Factor 1.6	Recht van bezwaar *Als in het privacy statement het recht op bezwaar wordt genoemd, wordt een punt toegekend.*	0-1 punt

Factor 1.7	Recht op beperking van gegevensverwerking *Als in het privacy statement het recht op beperking van gegevensverwerking wordt genoemd, wordt een punt toegekend. Ook wanneer er wordt gesproken van het uitsluiten van automatische verwerking wordt hier een punt toegekend.*	0-1 punt
Factor 1.8	Recht op vergetelheid *Als in het privacy statement het recht op vergetelheid wordt genoemd, wordt een punt toegekend. Als dit anders wordt genoemd, bijvoorbeeld 'verwijdering', wordt ook een punt toegekend.*	0-1 punt
Factor 1.9	Mogelijkheid klacht Autoriteit Persoonsgegevens *Als in het privacy statement de mogelijkheid tot het indienen van een klacht bij de Autoriteit Persoonsgegevens wordt genoemd, wordt een punt toegekend. Ook als er wordt verwezen naar de privacy autoriteit (in uw lidstaat), telt dit als een punt. De mogelijkheid om een klacht in te dienen is een vereiste voor een punt. Als er bijvoorbeeld enkel wordt gesproken over 'een melding', wordt geen punt toegekend.*	0-1 punt
Factor 1.10	Verwijzing naar privacy(verklaring) op homepage *Als op de homepage van een organisatie een link naar een pagina over privacy staat, wordt er een punt toegekend. Dit geldt voor links die direct naar de privacyverklaring verwijzen, maar ook voor links die verwijzen naar een pagina met algemene informatie over privacy.*	0-1 punt

Tabel 4 Factoren jaarverslagen

Jaarverslag		**Score**
Factor 2.1	Aantal woorden in jaarverslag besteed aan privacy *Het aantal woorden dat besteed wordt aan privacy wordt in het jaarverslag van 2018 gemeten. Woorden in alinea's die voornamelijk over privacy gaan worden volledig meegerekend. Als het over enkel een zin of een opsomming gaat waarin over privacy of GDPR wordt geschreven, worden alleen de woorden uit de zin meegeteld.* *Bij 300 of meer woorden wordt een punt toegekend.*	0-1 punt
Factor 2.2	Percentage van jaarverslag besteed aan privacy *Het aantal woorden dat bij factor 2.1 wordt gevonden wordt voor deze factor afgezet tegen het totaalaantal woorden van het jaarverslag. Van de jaarverslagen is het totaalaantal woorden met een factor van 0,9 berekend, om zo enigszins te compenseren voor niet relevante tekst in tabellen en rekeningen. Dit is voor alle jaarverslagen zo berekend dus onderling wordt over de organisaties geen voordeel gegeven.*	0-1 punt

	Als 0,5% of meer van de tekst over privacy en/of de GDPR gaat, wordt er een punt toegekend.	
Factor 2.3	Aantal hits op privacy/GDPR-trefwoorden in jaarverslag *In het jaarverslag wordt geteld hoe vaak de woorden 'privacy', 'AVG' en 'gegevensbescherming' voorkomen. Dit is een manier om te meten hoeveel aandacht er wordt besteed aan privacy en privacywetgeving als onderwerp. Voor Engelstalige jaarverslagen zijn de zoektermen 'privacy', 'GDPR' en 'data protection'.* *Er wordt een punt toegekend als er in het jaarverslag van 2018 meer dan 15 van de trefwoorden worden gevonden.*	0-1 punt
Factor 2.4	Ontwikkeling aantal trefwoorden ten opzichte van vorig jaar *Om te zien of de aandacht voor privacy en de GDPR zich heeft ontwikkeld tussen 2017 en 2018, wordt het verschil van factor 2.3 gemeten tussen de uitkomsten van de jaarverslagen uit 2017 en 2018.* *Wanneer er in het jaarverslag van 2018 sprake is dat de gezochte trefwoorden 5 keer of vaker voorkomen dan in het jaarverslag van 2017, wordt er een punt toegekend.*	0-1 punt
Factor 2.5	Verwijzing naar privacy statement in jaarverslag *Als er in het jaarverslag 2018 wordt verwezen naar het privacy statement, wordt een punt toegekend.*	0-1 punt

7.3.3. Ontbreken privacy statements en jaarverslagen

Als er geen privacy statement beschikbaar is van een organisatie, wordt gekeken of er op de website een pagina over privacy te vinden is. Als de informatie die wordt gevonden voldoet aan de factoren die worden beoordeeld in het privacy statement, worden de punten hiervan toegekend. Voor het ontbreken van een privacy statement wordt het punt voor aanwezigheid van een privacy statement vanzelfsprekend niet toegekend.

Als er geen jaarverslag beschikbaar is, is het niet mogelijk de factoren voor het jaarverslag te beoordelen en punten toe te kennen. In de statistische analyse wordt in deze gevallen een punt ingevuld om aan te geven dat de waarde ontbreekt.